UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

Aliaswire, Inc., Plaintiff, v. Branch Banking and Trust Company, and BB&T Corporation, Defendants.	)	Civil Action No. 6:19-cv-00648 **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff, Aliaswire, Inc. ("Aliaswire"), for its complaint against Defendants, Branch Banking and Trust Company and BB&T Corporation (collectively "BB&T"), hereby alleges as follows:

THE PARTIES

1. Aliaswire is a Delaware corporation having its principal place of business located at 152 Middlesex Turnpike, Burlington, Massachusetts 01803.

2. Upon information and belief BB&T Corporation ("BB&T Co.") is a North Carolina corporation doing business in this district with its headquarters located at 200 West Second St., Winston-Salem, North Carolina 27101. BB&T Co. is the parent company of Branch Banking and Trust Company which does business through approximately 123 financial centers across Texas, including at least 21 in this District. Upon information and belief, BB&T Co. may be

served with process through its registered agent CT Corporation System at 160 Mine Lack Ct. STE 200, Raleigh, North Carolina 27615.

3. Upon information and belief, Branch Banking and Trust Company, ("Branch Banking") is a North Carolina business corporation registered with the Texas Secretary of State to do business in Texas, with its headquarters located at 200 West Second St., Winston-Salem, North Carolina 27101. Branch Banking has regular and established places of business in this District including 21 branches in San Antonio, Austin and Bryan-College, for example 1313 SE Military Dr., San Antonio, Texas 78214; 106 South Saint Mary's Street, STE 100, San Antonio, Texas 78205; 803 Castroville Road, STE 322, San Antonio, Texas 78237, among others. Branch Banking is one of the 15 biggest banks in the State of Texas with approximately 5.3 billion in deposits statewide as of 2015. Branch Banking may be served with process through its registered agent, CT Corporation Systems, 1999 Bryan St., STE 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

4. This is a civil action for patent infringement under the patent laws of the United States, 35 U.S.C. § 271, *et seq.* This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has general personal jurisdiction over BB&T because BB&T is engaged in substantial and not isolated activity at its regular and established places of business within this judicial district. This Court has specific jurisdiction over BB&T because BB&T has committed acts of infringement giving rise to this action and has established more than minimum contacts within this judicial district, such that the exercise of jurisdiction over BB&T in this Court would not offend traditional notions of fair play and substantial justice.

6. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b)-(c) and 1400(b) because BB&T maintains regular and established places of business and has committed acts of patent infringement within this judicial district.

FACTUAL BACKGROUND

7. Aliaswire, Inc., was founded by Hossein Mohsenzadeh, a graduate of MIT's Sloan School of Business and Massachusetts resident. Hoss, as he often went by, created a user-friendly yet secure payment solution that was not limited by the ATM or private network of any one bank, and that did not require disclosing one's sensitive financial information to the other party or financial institution in order to facilitate the transfer of funds. Hoss' inventions subsequently became the linchpin of Burlington, Massachusetts based Aliaswire, which Hoss began in 2001 with no employees other than himself, and quickly grew to employ over 25 individuals.

8. Hoss realized that existing Transaction When Not Present ("TWNP") systems at the time posed a dilemma to a target customer (the transferee, or target) of a bank that was seeking to receive funds from a customer (the transferor) of another bank. Specifically, the transferee had to choose from among three flawed solutions. It could disclose all of its private financial information (e.g., bank account numbers) to the transferor, who could be a complete stranger. This option increased the risk of electronic fraud. The transferee could also sign up with a third-party payment service, with which the transferor is also registered, such as PayPal, that serves as a middle-man service between the transferor and the transferee. Like the first option, this second option required bank account information to be transferred to an entity besides the customer's bank (in this case, the sensitive information goes to the middle-man service such as PayPal or Venmo). This also came with an increased risk of fraud that would materialize, if for example, the middle-man service were to be hacked. This is not an insignificant risk, as evidenced for

example, by the middle-man service provider Tio Networks (then owned by PayPal) hack of 2017, where as many as 1.6 million customer's personal and financial information was stolen. *See, e.g., https://www.usatoday.com/story/tech/2017/12/04/paypal-acquired-company-reports-many-1-6-million-users-breached/919090001/.* This second option was also unacceptable, since it required the transferor and the transferee to sign up with the same third-party middle-man service (e.g., a Venmo user cannot send money to a PayPal user). If the first and second options were not acceptable, a third option would be for the transferee use more traditional methods of receiving funds, which sacrificed speed and ease of use.

9. Hoss' invention solved a problem specific to computer technology, i.e., how to reduce the potential for fraud in TWNP systems while more easily and more securely authenticating both parties to the transaction without disclosing private banking information. This problem is rooted in computer systems because it arises solely in the context of backend computer systems of financial institutions engaged in money-transfer transactions occurring over a communications network.

10. Hoss' system enabled banks to use aliases, that were more readily authenticated, but that were also themselves not particularly confidential, to more rapidly authenticate direct transfers of funds between one of their own customers and a customer at another trusted bank without requiring disclosure of confidential information. Because phone numbers and email addresses have already been semi-authenticated by wireless providers or service providers, in that when first established each is linked to a particular customer, they can serve as the basis for a secure yet convenient aliasing scheme as describe by Hoss.

11. BB&T's payment systems and solutions allows its customers to directly transfer funds to customers of other banks using a nationwide digital payments network run by most

American banks, including BB&T. That network is called "Zelle". Zelle integrates directly with BB&T's servers. The part of Zelle that serves BB&T's customers is maintained by BB&T itself. In this way, BB&T enables its Texas customers, including the ones residing in this district, to transfer funds to customers of other banks without having to disclose their private banking information to anyone outside their own bank.

THE PATENTS-IN-SUIT

12. On January 1, 2013, the Patent and Trademark Office (PTO) issued United States Patent No. 8,346,659 ("the '659 patent"), titled SECURE AUTHENTICATION AND PAYMENT SYSTEM. The '659 patent is presumed valid and enforceable. A copy of the '659 patent is attached as Exhibit A.

13. Aliaswire is the owner and assignee of all rights, title and interest in and to the '659 patent and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the '659 patent.

14. On June 20, 2017, the PTO issued United States Patent No. 9,684,899 ("the'899 patent"), titled SECURE AUTHENTICATION AND PAYMENT SYSTEM. The '899 patent is presumed valid and enforceable. A copy of the '899 patent is attached as Exhibit B.

15. Aliaswire is the owner and assignee of all rights, title and interest in and to the '899 patent and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the '899 patent.

16. On September 19, 2017, the PTO issued United States Patent No. 9,767,455 ("the '455 patent"), titled SECURE AUTHENTICATION AND PAYMENT SYSTEM. The '455 patent is presumed valid and enforceable. A copy of the '455 patent is attached as Exhibit C.

17. Aliaswire is the owner and assignee of all rights, title and interest in and to the '455 patent and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the '455 patent.

18. On November 13, 2018, the PTO issued United States Patent No. 10,127,550 ("the '550 patent"), titled SECURE AUTHENTICATION AND PAYMENT SYSTEM. The '550 patent is presumed valid and enforceable. A copy of the '550 patent is attached as Exhibit D.

19. Aliaswire is the owner and assignee of all rights, title and interest in and to the '550 patent and holds all substantial rights therein, including the right to grant licenses, to exclude others, and to enforce and recover past damages for infringement of the '550 patent.

20. On November 5, 2019, the PTO issued United States Patent No 10,467,621 ("the '621 patent"), titled SECURE AUTHENTICATION AND PAYMENT SYSTEM. The '621 patent is presumed valid and enforceable. A copy of the '621 patent is attached as Exhibit E.

21. The inventions of the '659 patent, '899 patent, '455 patent, '550 patent and '621 patent were invented by Hoss and later assigned to Aliaswire, Inc., the company he founded. Since inception, Aliaswire has been recognized as a leader in mobile/online payment processing and authentication. Hoss played a seminal role in the company's success.

COUNT I
(BB&T's Infringement of U.S. Patent No. 8,346,659)

22. Paragraphs 1-21 are reincorporated by reference as if fully set forth herein.

23. The elements claimed by the '659 patent, taken alone or in combination, were not well-understood, routine or conventional to one of ordinary skill in the art at the time of the invention. Rather, the '659 patent claims and teaches, *inter alia*, an improved system to process and authenticate a TWNP between an originator and a target. The invention improved upon then existing transaction authentication methods and systems, which were cumbersome, required

extensive disclosure of personal financial information, took several days to process and/or provided insufficient mechanisms by which an originating/target bank could verify individual transactions. The Hoss system uses an aliasing scheme through which party identity and transaction details could be verified and authenticated. This is accomplished by using unique alias information for each party, and a "facilitator" server containing such alias information and other non-sensitive transaction information, which could be used to verify the transaction in near real-time, without an originating bank or customer having to provide sensitive bank account and other financial information to a target bank or customer.

24. Instead of having to arrange a wire transfer by informing the originating bank of the target's name, bank account number, bank routing number, address, target bank name etc., a consumer or business wishing to transfer funds to a target customer or business simply had to provide an originator and target alias that could be authenticated by the facilitator server, but that was itself not sensitive financial information that the target/originator wishes to keep confidential. Upon authentication by one of the member banks, that bank provided a guarantee that the transaction was valid, which meant that the funds could be made available substantially immediately, dispensing with the need for sensitive disclosures and complicated and lengthy approval processes, while also providing increased security.

25. Compared to the prior art, the claimed system for payment authentication and processing is more resilient against fraud because nothing is exchanged during the transaction process that could increase the risk of unauthorized transfers. The alias used to facilitate transfers in Hoss' system, which could be an email address or phone number, by itself cannot be used to facilitate unauthorized transfers. Hoss' system uses an aliasing database which requires only non-sensitive information to be exchanged over the communications network and reconciles transfer

details using confidential information that is handled only by the customer's own bank. Such a system is highly resistant to man-in-the-middle attacks and/or spoofing. Thus, Hoss' invention improved TWNP systems by the use of such aliases, allowing for smaller more efficient databases in place of large and disparate institution specific databases, as well as avoiding interoperability issues between previously proprietary transaction systems.

26. The invention represented a technical solution to an unsolved technological problem. The written description of the '659 patent describes, in technical detail, each of the limitations in the claims, allowing a person of skill in the art to understand what those limitations cover, and therefore what was claimed, and to also understand how the non-conventional and non-generic ordered combination of the elements of the claims differ markedly from what had been conventional or generic in the industry at the time of the inventions of the '659 patent.

27. For instance, the claims cover a specific and discrete way to address the problem of reducing fraud and more easily and more securely authenticating transactions in TWNP systems. The invention's solution to this problem is a system that replaces use of private banking information with machine-generated and pre-authenticated aliases to authorize and initiate the transaction directly between financial institutions.

28. More particularly, the inventions disclosed in the '659 patent include transforming non-sensitive user identifying information into an encoded alias which can be efficiently stored in a shared database that is accessible by a number of banks nationwide. The non-sensitive alias information is used by a transferor bank customer (the originator) to identify itself and recipient of transfer requests (e.g., by providing a party alias). When payment is sent to a customer of a bank that has integrated the shared database, the alias is used to authenticate the originator and the recipient by matching the information received by the originator or recipient with the identification

stored in the specialized "alias" database. In this manner, financial institutions are assured that the originator and recipient are authorized users. Thereafter, the banks can facilitate the transfer in near real-time, using existing electronic fund transfer technologies, with limited risk that the transaction is fraudulent, and without forcing one customer to share its confidential banking information with the other customer. Moreover, from the user's perspective, the process is unobtrusive, fast and convenient, improving user adoption while still providing increased security. While having wide-ranging implications for the financial industry, the solutions described in the '659 patent are narrowly tailored to the specific fund transfer problems identified above, and thus do not preempt the entire field of securely transferring funds without requiring a transferee customer to share its sensitive financial information with a transferor customer.

29. The claims of the '659 patent each recite authenticating that an originator (transferor) is authorized to conduct a transaction (transfer funds) based on a comparison with previously stored credentials in an authorized user database. Receiving at a server one or more messages including an alias and payment amount; retrieving financial account information (e.g., indication of receiving bank/financial institution) relating to the target (transferee) stored in said database, and based on the originator and target information sent to/received at the server, providing instructions to transfer the desired sum.

30. The system covered by the asserted claims differs markedly from the conventional and generic systems in use at the time of this invention, which *inter alia* lacked the claimed combination of authorized user database, aliasing information, authenticating base upon comparison of said alias information in a database and instructing funds to be transferred from one financial account to another.

31. The ‘659 patent is drawn to solving the specific, technical problem of reducing the potential for fraud in TWNP systems while more easily and more securely authenticating the transaction, particularly in a mobile computing environment and/or over a public communications network, without the disclosure of private banking information. Consistent with the problem addressed being rooted in such TWNP systems, the ‘659 patent’s solutions of replacing private banking information with machine generated, pre-authenticated aliases to facilitate a direct transfer between financial institutions are also rooted in that same technology and cannot be performed with pen and paper or in the human mind. For example, a human cannot use a machine generated alias, which requires a specific sequence of numeric or alpha-numeric characters to identify a desired transferee, never mind authenticate the transaction directly to that transferee’s financial institution without requiring the transferee to disclose its private banking information outside of its financial institution.

32. As noted in the patent’s specification, the invention’s benefits include removing the inherent susceptibility of fraud in communications via public data networks, such as the Internet; reducing the computing power and complexity required for authentication where very large institution specific databases were previously used; and enabling near real-time money transfers directly between financial institutions that maintain private banking networks incapable of integrating with each other.

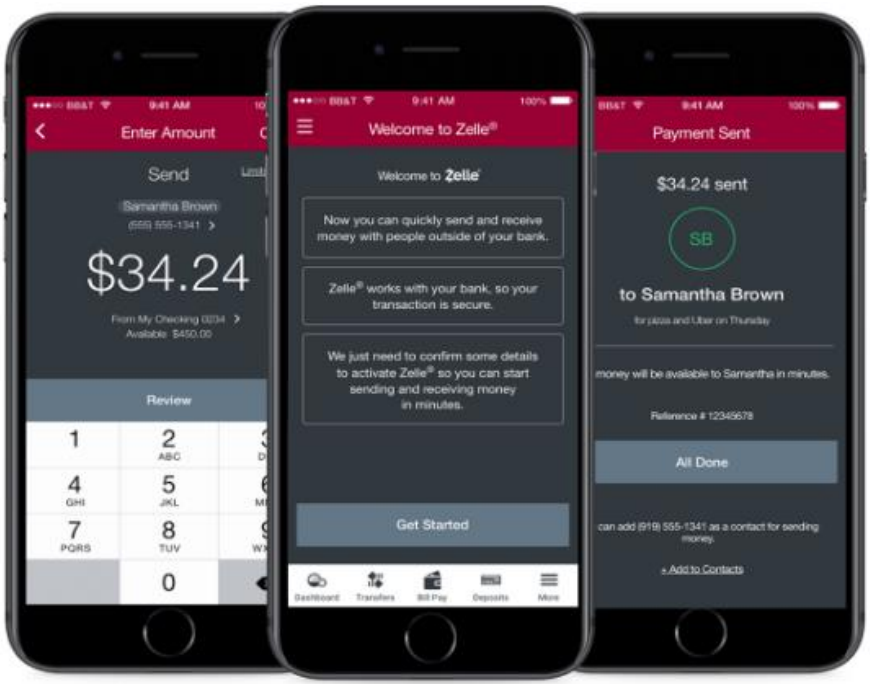
33. BB&T has directly infringed, and continues to directly infringe, literally and/or by the doctrine of equivalents, individually and/or jointly, at least claims 1 and 31 of the ‘659 patent by making, using, testing, selling, offering for sale and/or importing into the United States products and/or services covered by one or more claims of the ‘659 patent. BB&T’s products and/or services that infringe the ‘659 patent include, but are not limited to, its “U” mobile application P2P

payment system referred to as "Send Money with Zelle", and any other BB&T products and/or services, either alone or in combination, that operate in substantially the same manner.

34. Claim 1 of the '659 patent is reproduced below:

> 1. A method of conducting a financial transaction between an originator and a target comprising:
>
> authenticating that the originator is authorized to conduct the said financial transaction based on credentials previously stored in an authorized user database;
>
> receiving at a server one or more messages that include at least an alias and a payment amount;
>
> retrieving target financial account information previously stored from a database based on the said alias;
>
> providing instructions to transfer the payment amount from an originator financial account to a target financial account by the server based on target financial account information identified by the alias.

35. BB&T's mobile banking smartphone application "U" in combination with BB&T's backend servers as integrated with the Zelle Alias Directory performs a method of conducting a financial transaction between an originator and a target as claimed in the '659 patent. For example, the BB&T "send money with Zelle" P2P payment function enables sending money (financial transaction) from an initiator's BB&T bank account (originator) to a recipient's bank account (target), as illustrated below:



How to get started

You can enroll with *Zelle* through U by BB&T® online banking or mobile app in three simple steps.

1. Select Send Money with ***Zelle*** in the U navigation menu
2. Choose the primary account you want to use for *Zelle* payments
3. Verify your contact information (U.S. mobile number and/or email) for payments

Enroll with *Zelle* now by logging in to U.

Log in →

How Zelle works

Simply select or add contacts, enter the amount you wish to send, review and select Send.

If your contact already uses *Zelle*, they'll receive their payment within minutes. [1] If not, they'll receive a notification with instructions on how to enroll.

When using *Zelle*, be sure to have the correct contact information, and treat *Zelle* the same as sending cash.

Send money in 3 easy steps

Zelle is a simple and secure way to send and receive money:

1. Log in to U with your online banking user ID and password
2. Select Send Money with ***Zelle*** in the U navigation menu
3. Select Send

Once enrolled, customers can send, request, or receive money with Zelle. To initiate a transaction, users enter the recipient's email address or phone number and the amount to be sent or requested. Users also have the option to add a memo line to the transaction.

36. Following the above example, BB&T authenticates the initiating party (originator) based on credentials stored in a customer database (authorized user database):

Network Directory—
In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

6. Enrolling in the Service

a. You must provide us with an email address that you regularly use and intend to use regularly (i.e., no disposable email addresses) and a permanent mobile phone number that you intend to use for an extended period of time (i.e., no "burner" numbers).

Mobile Phone Number – When shared with us, we collect your mobile number as a means for communicating payment notifications to you and also as a token for authenticating your identity. We also collect the mobile number of any individual which you provide to us for the purpose of facilitating money transfers.

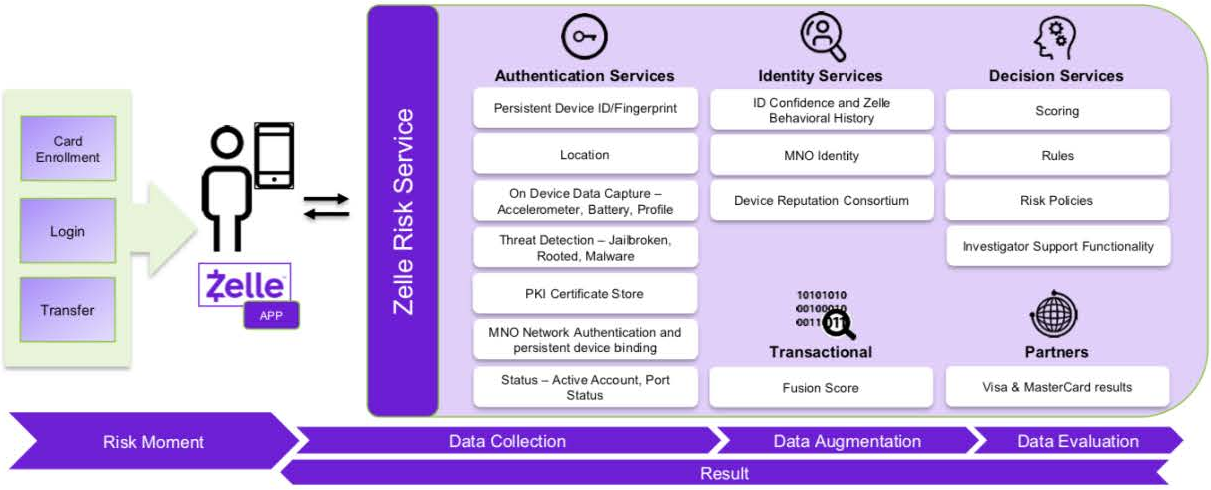
Email Address – We collect your email address when you register an account and to provide you notifications regarding payment transfers and also as a token for authenticating your identity. We also collect the email address of any individual which you provide to us for the purpose of facilitating money transfers.

37. Furthermore, when the originator has been authenticated as an authorized user, BB&T's backend servers as integrated with the Zelle Alias Directory receive message(s) including an alias representing the desired recipient (e.g., email address, telephone number, token, etc.) and the amount to be transferred:

Security—
Zelle was developed by the banking industry and benefits from the industry's cybersecurity expertise. Financial institutions in the network do not share customers' account information with each other, so the risk of account information being captured in-flight or at rest is decreased. Customers that access Zelle through their bank's mobile app need provide no sensitive account information. Those who use the standalone app need only share debit card information. The Zelle Alias directory used to facilitate payments only includes the phone numbers and emails associated with Zelle profiles.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

Recipient information refers to information about a recipient used to properly direct payment to the recipient and permit the recipient to identify the correct recipient account.



Sender identifies the name of recipient, recipient's cell phone or email address (each a "token"), and the amount of the payment. (Name not used for verification purposes.)

38. BB&T's backend servers as integrated with the Zelle Alias Directory (database) further retrieve information indicating the recipient's financial institution and/or that it has a valid

pay-to account (target financial account information), which is associated with the previously received target alias (e.g., email address, telephone number, token, etc.):

In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

Zelle **maintains a database of information and through the Service provides the Network Financial Institutions with information necessary to facilitate the transfer of money ("Messages"); however,** ***Zelle*** **neither transfers, moves nor initiates the transfer or movement of money.** *Zelle*

6. Enrolling in the Service

a. You must provide us with an email address that you regularly use and intend to use regularly (i.e., no disposable email addresses) and a permanent mobile phone number that you intend to use for an extended period of time (i.e., no "burner" numbers).

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

39. BB&T's backend servers as integrated with the Zelle Alias Directory also provide instructions to transfer the indicated funds from the initiator's "pay-from" account (originator financial account) to the recipient's financial institution and/or "pay-to" account (target financial account) based on the indication of a valid "pay-to" account being associated with the initiator's alias as described above:

You may send money to another User at your initiation or in response to that User's request for money. You understand that use of this Service by you shall at all times be subject to (i) this Service Agreement, (ii) your express authorization for a Network Financial Institution to initiate a debit entry to your bank account, and (iii) the terms and conditions of your account agreement with your financial institution. You understand that when you send the payment, you will have no ability to stop it. You

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

- The member bank transmits inquiry to EWS to determine if recipient's token is in a "shared directory."
- Assume recipient is not in the directory.
- EWS informs the member bank that recipient's token is not in the shared directory. (If recipient is in the directory, payment is available same day, virtually in real time.)

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

40. Additionally, BB&T has been, and currently is, an active inducer of infringement of the '659 patent under 35 U.S.C. § 271(b) and contributory infringement of the '659 patent under 35 U.S.C. § 271(c) literally and/or by the doctrine of equivalents.

41. With knowledge of the '659 patent, BB&T has actively induced, and continues to actively induce, infringement of the '659 patent by intending that others use, offer for sale, or sell in the United States, products and/or services covered by one or more claims of the '659 patent, including but not limited to BB&T's "U" mobile application P2P functionality as integrated with Zelle, and any BB&T product and/or service, alone or in combination, that operates in materially the same manner. BB&T provides such products and/or services to others, such as customers,

who, in turn, use, provision for use, offer for sale, or sell in the United States products and/or services that directly infringe one or more claims of the '659 patent.

42. BB&T has actual knowledge of the '659 patent since at least as early as the service upon BB&T of this Complaint. By the time of trial, BB&T will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '659 patent.

43. BB&T has committed, and continues to commit, affirmative acts that cause infringement of one or more claims of the '659 patent with knowledge of the '659 patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '659 patent. BB&T induces such acts of infringement by its affirmative actions of intentionally providing software components that when used in their normal and customary way as desired and intended by BB&T, infringe one or more claims of the '659 patent and/or by directly or indirectly providing instructions on how to use its products and/or services in a manner or configuration that infringes one or more claims of the '659 patent, including those found at one or more of the following:

- https://www.bbt.com/online-access/online-banking/send-money-with-zelle.html
- https://www.bbt.com/online-access/online-banking/u-by-bbt-video-demos.html
- https://www.bbt.com/online-access/mobile-banking.html
- https://apps.apple.com/us/app/u-digital-banking/id995112030
- https://www.bbt.com/online-access/mobile-banking/mobile-faq.html

44. BB&T has also contributed to, and continues to contribute to, the infringement of the '659 patent by others by knowingly providing products and/or services that, when installed and configured result in a system as intended by BB&T, directly infringe one or more claims of the

‘659 patent by a third party, and which have no substantial non-infringing uses, or include a separate and distinct software module described above that is especially made or especially adapted for use in infringement of the ‘659 patent and is not a staple article or commodity of commerce suitable for substantial non-infringing use.

45. As a result of BB&T’s acts of infringement, Plaintiff has suffered and will continue to suffer damages in an amount to be proved at trial.

COUNT II
(BB&T’s Infringement of U.S. Patent No. 9,684,899)

46. Paragraphs 1-45 are reincorporated by reference as if fully set forth herein.

47. The elements claimed by the ‘899 patent, taken alone or in combination, were not well-understood, routine or conventional to one of ordinary skill in the art at the time of the invention. Rather, the ‘899 patent claims and teaches, *inter alia*, an improved way to process and authenticate a Transaction When Not Present (“TWNP”) between two parties. The invention improved upon then existing transaction authentication methods and systems, which were cumbersome, required extensive disclosure of personal financial information, took several days to process and/or provided insufficient mechanisms by which an originating/target bank could verify individual transactions, with an aliasing scheme through which party identity and transaction details could be verified and authenticated.

48. The invention further improved upon prior systems and methods by providing a mechanism whereby even a target (e.g., recipient) not previously registered with a payment network could receive transferred funds. This was accomplished by using a unique alias for each party and a “facilitator” server containing alias information and other non-sensitive transaction information which could be used to verify the transaction in near real-time, without an originator

or target having to provide its sensitive bank account and other financial information outside of its financial institution.

49. In the event of an intended target not being registered with a payment network, the invention teaches a system and method by which the target is notified of the pending transfer and provided instructions to retrieve the transferred funds, again, without disclosing secure financial information outside of the recipient's financial institution.

50. Instead of having to arrange a wire transfer by informing the originating bank of the target's name, bank account number, bank routing number, address, target bank name etc., a consumer or business wishing to transfer funds to a target customer or business simply had to provide an originator and target alias and other non-sensitive information to be authenticated by the facilitator server, but that was itself not sensitive financial information that the target/originator wishes to keep confidential. Upon authentication by one or both of the member banks, that bank was provided a guarantee that the transaction was valid, and the funds could be made available substantially immediately, thereby dispensing with the need for sensitive disclosures and complicated and lengthy approval processes, while also providing increased security.

51. Compared to the prior art, the claimed system for payment authentication and processing is more resilient against fraud because nothing is exchanged during the transaction process that could increase the risk of unauthorized transfers. The alias used to facilitate transfers in Hoss' system, which could be an email address or phone number for example, by itself cannot be used to facilitate unauthorized transfers. Hoss' system uses an aliasing database which requires only non-sensitive information to be exchanged over the communications network and reconciles transfer details using confidential information that is handled only by the customer's own bank. Such a system is highly resistant to man-in-the-middle attacks and/or spoofing.

52. The invention represented a technical solution to an unsolved technological problem. The written description of the '899 patent describes, in technical detail, each of the limitations in the claims, allowing a person of skill in the art to understand what those limitations cover, and therefore what was claimed, and to also understand how the non-conventional and non-generic ordered combination of the elements of the claims differ markedly from what had been conventional or generic in the industry at the time of the inventions of the '899 patent.

53. For instance, the inventions disclosed in the '899 patent include transforming non-sensitive user identifying information into an encoded alias which can be efficiently stored in a shared database that is accessible by a number of banks nationwide. The non-sensitive alias information is used by a transferor bank customer (the originator) to identify itself and recipient of transfer requests (e.g., by providing a party alias). When payment is sent to a customer of a bank that has integrated the shared database, the alias is used to authenticate the originator and the recipient by matching the information received by the originator or recipient with the identification stored in the specialized "alias" database. In this manner, financial institutions are assured that the originator and recipient are authorized users. Thereafter, the banks can facilitate the transfer in near real-time, using existing electronic fund transfer technologies, with limited risk that the transaction is fraudulent, and without forcing one customer to share its confidential banking information with the other customer. Moreover, from the user's perspective, the process is unobtrusive, fast and convenient, improving user adoption while still providing increased security. While having wide-ranging implications for the financial industry, the solutions described in the '899 patent are narrowly tailored to the specific fund transfer problems identified above, and thus do not preempt the entire field of securely transferring funds without requiring a transferee customer to share its sensitive financial information with a transferor customer.

54. More specifically, the claims of the '899 patent recite sending from a server to a client device a message using an alias previously assigned by the server and stored in a database, where the message provides instructions for a target (recipient/transferee) to access the server to receive a payment amount. Further, the claims of the '899 patent recite receiving, at the server from the client device, one or more messages including an alias and a transaction identifier from the target for the transaction; authenticating, by the server, the one or more messages by searching for the previously stored alias and transaction identifier associated with the alias in the database that matches the received alias and transaction identifier; where the alias identifies a party to the transaction and the transaction identifier identifies the transaction.

55. Certain embodiments of the invention also include target financial account information being received at the server; linking the target financial account information to the alias stored in the database; and in response to the authenticating, providing instructions to transfer the payment from an originator financial account to a target financial account.

56. The system covered by the asserted claims differs markedly from the conventional and generic systems in use at the time of this invention, which *inter alia* lacked the claimed combination of facilitating server, previously assigned alias, generated transaction identifier, instructions for a target to receive the payment, and authentication based on matching received and previously stored alias and transaction identifier.

57. The '899 patent is drawn to solving the specific, technical problem of reducing the potential for fraud in TWNP systems while more easily and more securely authenticating the transaction, particularly in a mobile computing environment and/or over a public communications network, without the disclosure of private banking information. Consistent with the problem addressed being rooted in such TWNP systems, the '899 patent's solutions of replacing private

banking information with machine generated, pre-authenticated aliases to facilitate a direct transfer between financial institutions are also rooted in that same technology and cannot be performed with pen and paper or in the human mind. For example, a human cannot use a machine generated alias, which requires a specific sequence of numeric or alpha-numeric characters to identify a desired transferee, never mind authenticate the transaction directly to that transferee's financial institution without requiring the transferee to disclose its private banking information outside of its financial institution.

58. As noted in the patent's specification, the invention's benefits include removing the inherent susceptibility to fraud in communications via public data networks, such as the Internet; reducing the computing power and complexity required for authentication where very large institution specific databases were previously used; and enabling near real-time money transfers directly between financial institutions that maintain private banking networks incapable of integrating with each other.

59. BB&T has directly infringed, and continues to directly infringe, literally and/or by the doctrine of equivalents, individually and/or jointly, at least claims 10, 11-12 and 15 of the '899 patent by making, using, testing, selling, offering for sale and/or importing into the United States products and/or services covered by one or more claims of the '899 patent. BB&T's products and/or services that infringe the '899 patent include, but are not limited to, its "U" mobile application P2P payment system referred to as "Send Money with Zelle", and any other BB&T products and/or services, either alone or in combination, that operate in substantially the same manner.

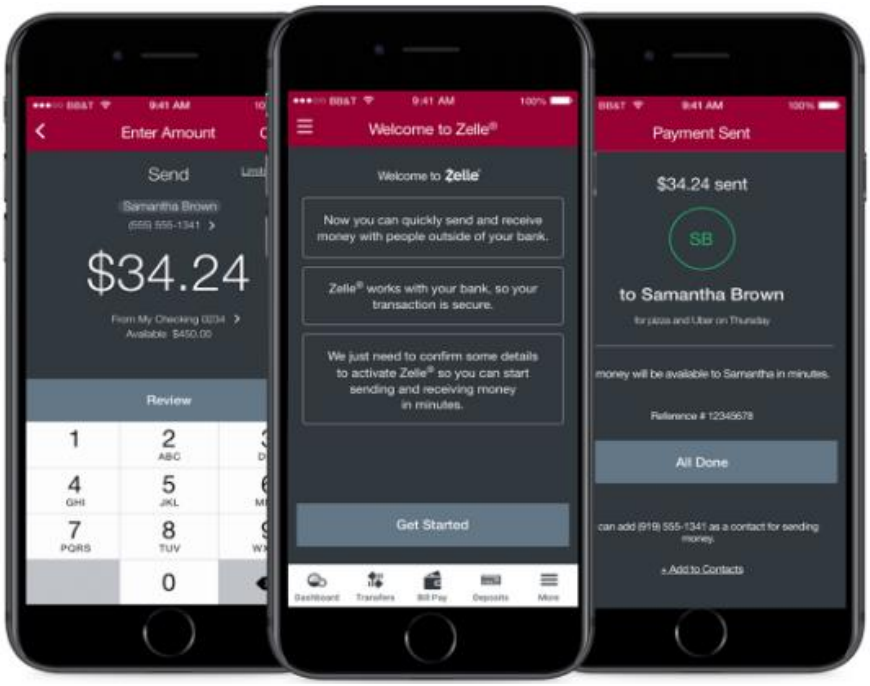
60. Claim 10 of the '899 patent is reproduced below:

10. A method comprising:

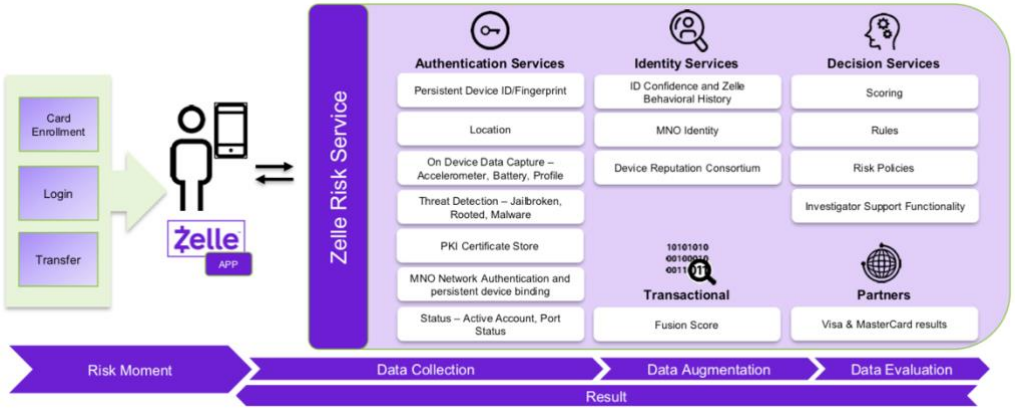
> sending, from a server, a message to a client device using an alias previously assigned by the server and stored in a database, wherein the message provides instructions for a target to access the server to receive a payment amount for a transaction and the message includes a transaction identifier generated for the transaction;
>
> receiving, at the server from the client device, one or more messages including at least an alias and the transaction identifier from the target for the transaction; and
>
> authenticating, by the server, the one or more messages from the client device by searching for the previously stored alias and the generated transaction identifier associated with the alias in the database that matches the received alias and the received transaction identifier in the one or more messages,
>
> wherein the alias identifies a party to the transaction and the transaction identifier identifies the transaction.

61. BB&T's mobile banking smartphone application in combination with BB&T's backend servers as integrated with the Zelle Alias Directory performs a method comprising sending, from a server, a message to a client device using an alias previously assigned by the server and stored in a database, wherein the message provides instructions for a target to access the server to receive payment and includes a generated transaction identifier, as claimed in the '899 patent.

62. For example, the BB&T "U" mobile application's "send money with Zelle" P2P payment function provides for an initiating transferor to send funds to a recipient transferee via the BB&T backend servers as integrated with Zelle. The BB&T backend servers as integrated with Zelle Alias Directory can operate to store an alias for the target along with a transaction identifier, and further, send a message with instructions regarding accessing the transfer to the transferee's client device (e.g., mobile phone) as illustrated below:



If you are sending money to someone who has not enrolled as a User with *Zelle*, either in the *Zelle* mobile app or with a Network Financial Institution, they will receive a text message or email notification instructing them on how to enroll with *Zelle* to receive the money. You understand and acknowledge that a



Will the person I send money to be notified?

Yes! They will receive a notification via email or text message. The message may be sent by *Zelle* or by their bank or credit union.

63. BB&T's backend servers as integrated with the Zelle Alias Directory receives one or more messages from the client device (e.g., transferee's mobile phone) which includes an alias for the target and the transaction identifier generated when the transferor submitted the transfer request:

Network Directory—
In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

6. Enrolling in the Service

a. You must provide us with an email address that you regularly use and intend to use regularly (i.e., no disposable email addresses) and a permanent mobile phone number that you intend to use for an extended period of time (i.e., no "burner" numbers).

The member bank transmits inquiry to EWS to determine if recipient's token is in a "shared directory."
Assume recipient is not in the directory.
EWS informs the member bank that recipient's token is not in the shared directory. (If recipient is in the directory, payment is available same day, virtually in real time.)
The member bank contacts recipient through the token advising the recipient of the pending transfer by sender and requesting recipient to enroll in the service through recipient's bank (if that bank offers the Zelle payment service) or with EWS.
If recipient banks with a network member bank, recipient may enroll in Zelle through that bank.

If you are sending money to someone who has not enrolled as a User with *Zelle*, either in the *Zelle* mobile app or with a Network Financial Institution, they will receive a text message or email notification instructing them on how to enroll with *Zelle* to receive the money. You understand and acknowledge that a

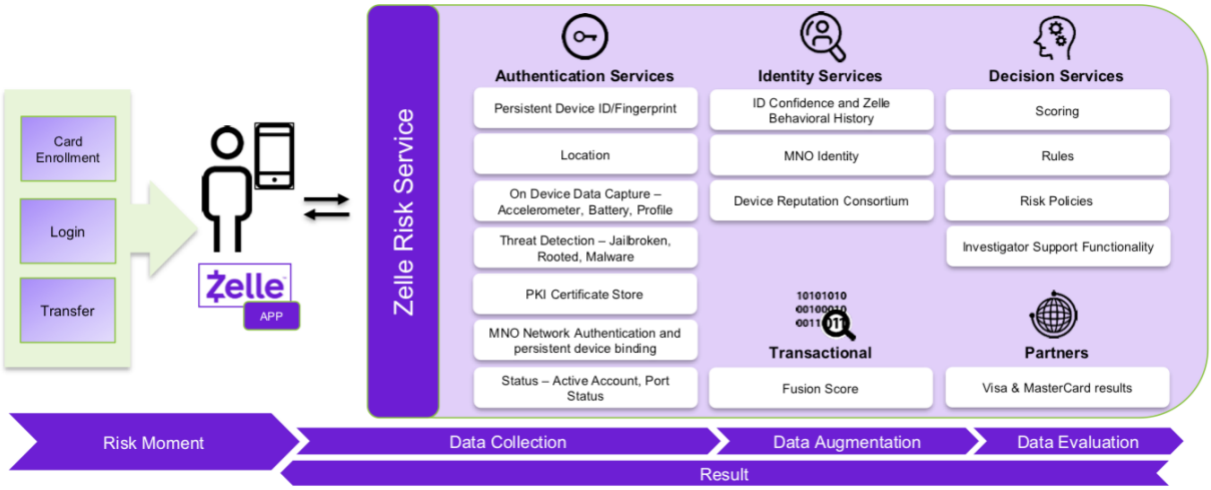
64. Furthermore, the BB&T backend as integrated with the Zelle Alias Directory authenticates the one or more messages from the client device by searching for the alias and transaction identifier in the database that matches the alias and transaction identifier received from the client device:

Security—

Zelle was developed by the banking industry and benefits from the industry's cybersecurity expertise. Financial institutions in the network do not share customers' account information with each other, so the risk of account information being captured in-flight or at rest is decreased. Customers that access Zelle through their bank's mobile app need provide no sensitive account information. Those who use the standalone app need only share debit card information. The Zelle Alias directory used to facilitate payments only includes the phone numbers and emails associated with Zelle profiles.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

Recipient information refers to information about a recipient used to properly direct payment to the recipient and permit the recipient to identify the correct recipient account.



Mobile Phone Number – When shared with us, we collect your mobile number as a means for communicating payment notifications to you and also as a token for authenticating your identity. We also collect the mobile number of any individual which you provide to us for the purpose of facilitating money transfers.

Email Address – We collect your email address when you register an account and to provide you notifications regarding payment transfers and also as a token for authenticating your identity. We also collect the email address of any individual which you provide to us for the purpose of facilitating money transfers.

65. In addition, the alias identifies the target transferee (party to the transaction) and the transaction identifier identifies the particular transaction:

In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

8. Receiving Money; Money Transfers by Network Banks

Once a User initiates a transfer of money to your email address or mobile phone number registered with the Service, you have no ability to stop the transfer. By using the Service, you agree and authorize us to initiate credit entries to the bank account you have registered.

6. Enrolling in the Service

a. You must provide us with an email address that you regularly use and intend to use regularly (i.e., no disposable email addresses) and a permanent mobile phone number that you intend to use for an extended period of time (i.e., no "burner" numbers).

66. Additionally, BB&T has been, and currently is, an active inducer of infringement of the '899 patent under 35 U.S.C. § 271(b) and contributory infringement of the '899 patent under 35 U.S.C. § 271(c) literally and/or by the doctrine of equivalents.

67. With knowledge of the '899 patent, BB&T has actively induced, and continues to actively induce, infringement of the '899 patent by intending that others use, offer for sale, or sell in the United States, products and/or services covered by one or more claims of the '899 patent,

including but not limited to BB&T's "U" mobile application P2P functionality as integrated with Zelle, and any BB&T product and/or service, alone or in combination, that operates in materially the same manner. BB&T provides such products and/or services to others, such as customers, who, in turn, use, provision for use, offer for sale, or sell in the United States products and/or services that directly infringe one or more claims of the '899 patent.

68. BB&T has actual knowledge of the '899 patent since at least as early as the service upon BB&T of this Complaint. By the time of trial, BB&T will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '899 patent.

69. BB&T has committed, and continues to commit, affirmative acts that cause infringement of one or more claims of the '899 patent with knowledge of the '899 patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '899 patent. BB&T induces such acts of infringement by its affirmative actions of intentionally providing software components that when used in their normal and customary way as desired and intended by BB&T, infringe one or more claims of the '899 patent and/or by directly or indirectly providing instructions on how to use its products and/or services in a manner or configuration that infringes one or more claims of the '899 patent, including those found at one or more of the following:

- https://www.bbt.com/online-access/online-banking/send-money-with-zelle.html
- https://www.bbt.com/online-access/online-banking/u-by-bbt-video-demos.html
- https://www.bbt.com/online-access/mobile-banking.html
- https://apps.apple.com/us/app/u-digital-banking/id995112030
- https://www.bbt.com/online-access/mobile-banking/mobile-faq.html

70. BB&T has also contributed to, and continues to contribute to, the infringement of the '899 patent by others by knowingly providing products and/or services that, when installed and configured result in a system as intended by BB&T, directly infringe one or more claims of the '899 patent by a third party, and which have no substantial non-infringing uses, or include a separate and distinct software module described above that is especially made or especially adapted for use in infringement of the '899 patent and is not a staple article or commodity of commerce suitable for substantial non-infringing use.

71. As a result of BB&T's acts of infringement, Plaintiff has suffered and will continue to suffer damages in an amount to be proved at trial.

COUNT III
(BB&T's Infringement of U.S. Patent No. 9,767,455)

72. Paragraphs 1-71 are reincorporated by reference as if fully set forth herein.

73. The elements claimed by the '455 patent, taken alone or in combination, were not well-understood, routine or conventional to one of ordinary skill in the art at the time of the invention. Rather, the '455 patent claims and teaches, *inter alia*, an improved way to process and authenticate a TWNP between parties. The invention improved upon then existing transaction authentication methods and systems, which were cumbersome, required extensive disclosure of personal financial information, took several days to process and/or provided insufficient mechanisms by which an originating/target bank could verify individual transactions, with an aliasing scheme through which party identity and transaction details could be verified and authenticated. This is accomplished by using a unique telephone identifier and alias to identify a transferee/recipient, transaction identifier, resource identifier, as well as a "facilitator" server containing alias information and other non-sensitive transaction information which could be used

to verify the transaction in near real-time, without an originating bank or customer having to provide sensitive bank account and other financial information to a target bank or customer.

74. Instead of having to arrange a wire transfer by informing the originating bank of the target's name, bank account number, bank routing number, address, target bank name etc., a consumer or business wishing to transfer funds to a target customer or business (transferee/recipient) simply had to provide the party's telephone number, alias and resource identifier that could be authenticated by the facilitator server, but that was itself not sensitive financial information that the target/originator wishes to keep confidential. Upon authentication by one of the member banks, that bank provided a guarantee that the transaction was valid, and the funds could be made available substantially immediately, thereby dispensing with the need for sensitive disclosures and complicated and lengthy approval processes.

75. Compared to the prior art, the claimed system for payment authentication and processing is more resilient against fraud because nothing is exchanged during the transaction process that could increase the risk of unauthorized transfers. The alias used to facilitate transfers in Hoss' system, which could be an email address or phone number, by itself cannot be used to facilitate unauthorized transfers. Hoss' system uses an aliasing database which requires only non-sensitive information to be exchanged over the communications network and reconciles transfer details using confidential information that is handled only by the customer's own bank. Such a system is highly resistant to man-in-the-middle attacks and/or spoofing. Thus, Hoss' invention improved TWNP systems by the use of such aliases, allowing for smaller more efficient databases in place of large and disparate institution specific databases, as well as avoiding interoperability issues between previously proprietary transaction systems.

76. The invention represented a technical solution to an unsolved technological problem. The written description of the '455 patent describes, in technical detail, each of the limitations in the claims, allowing a person of skill in the art to understand what those limitations cover, and therefore what was claimed, and to also understand how the non-conventional and non-generic ordered combination of the elements of the claims differ markedly from what had been conventional or generic in the industry at the time of the inventions of the '455 patent.

77. For instance, the claims cover a specific and discrete way to address the problem of reducing fraud and more easily and more securely authenticating transactions in TWNP systems. The invention's solution to this problem is a system that replaces use of private banking information with machine-generated and pre-authenticated aliases to authorize and initiate the transaction directly between financial institutions.

78. More particularly, the inventions disclosed in the '455 patent include transforming non-sensitive user identifying information into an encoded alias which can be efficiently stored in a shared database that is accessible by a number of banks nationwide. The non-sensitive alias information is used by a transferor bank customer (the originator) to identify itself and recipient of transfer requests (e.g., by providing a party alias). When payment is sent to a customer of a bank that has integrated the shared database, the alias is used to authenticate the originator and the recipient by matching the information received by the originator or recipient with the identification stored in the specialized "alias" database. In this manner, financial institutions are assured that the originator and recipient are authorized users. Thereafter, the banks can facilitate the transfer in near real-time, using existing electronic fund transfer technologies, with limited risk that the transaction is fraudulent, and without forcing one customer to share its confidential banking information with the other customer. Moreover, from the user's perspective, the process is

unobtrusive, fast and convenient, improving user adoption while still providing increased security. While having wide-ranging implications for the financial industry, the solutions described in the '455 patent are narrowly tailored to the specific fund transfer problems identified above, and thus do not preempt the entire field of securely transferring funds without requiring a transferee customer to share its sensitive financial information with a transferor customer.

79. The claims of the '455 patent recite receiving, at a server from a client device (e.g., mobile phone), one or more messages including a resource identifier, telephone identifier, and alias assigned by the server. Transforming, by the server, the telephone identifier and the alias from a message structure to a database structure; authenticating, by the server, the message by searching for a stored alias and transaction identifier associated with the alias in a database that matches the alias and telephone identifier; and in response to authenticating, authorizing a transfer of resources.

80. The system covered by the asserted claims differs markedly from the conventional and generic methods in use at the time of this invention, which *inter alia* lacked the claimed combination of telephone identifier, resource identifier, transaction identifier, aliasing information, authenticating base upon matching said alias, telephone identifier and transaction identifier from a database, and authorizing the transfer in response.

81. The '455 patent is drawn to solving the specific, technical problem of reducing the potential for fraud in TWNP systems while more easily and more securely authenticating the transaction, particularly in a mobile computing environment and/or over a public communications network, without the disclosure of private banking information. Consistent with the problem addressed being rooted in such TWNP systems, the '455 patent's solutions of replacing private banking information with machine generated, pre-authenticated aliases to facilitate a direct transfer

between financial institutions are also rooted in that same technology and cannot be performed with pen and paper or in the human mind. For example, a human cannot use a machine generated alias, which requires a specific sequence of numeric or alpha-numeric characters to identify a desired transferee, never mind authenticate the transaction directly to that transferee's financial institution without requiring the transferee to disclose its private banking information outside of its financial institution.

82. As noted in the patent's specification, the invention's benefits include removing the inherent susceptibility of fraud in communications via public data networks, such as the Internet; reducing the computing power and complexity required for authentication where very large institution specific databases were previously used; and enabling near real-time money transfers directly between financial institutions that maintain private banking networks incapable of integrating with each other.

83. BB&T has directly infringed, and continues to directly infringe, literally and/or by the doctrine of equivalents, individually and/or jointly, at least claim 1 of the '455 patent by making, using, testing, selling, offering for sale and/or importing into the United States products and/or services covered by one or more claims of the '455 patent. BB&T's products and/or services that infringe the '455 patent include, but are not limited to, its "U" mobile application P2P payment system referred to as "Send Money with Zelle", and any other BB&T products and/or services, either alone or in combination, that operate in substantially the same manner.

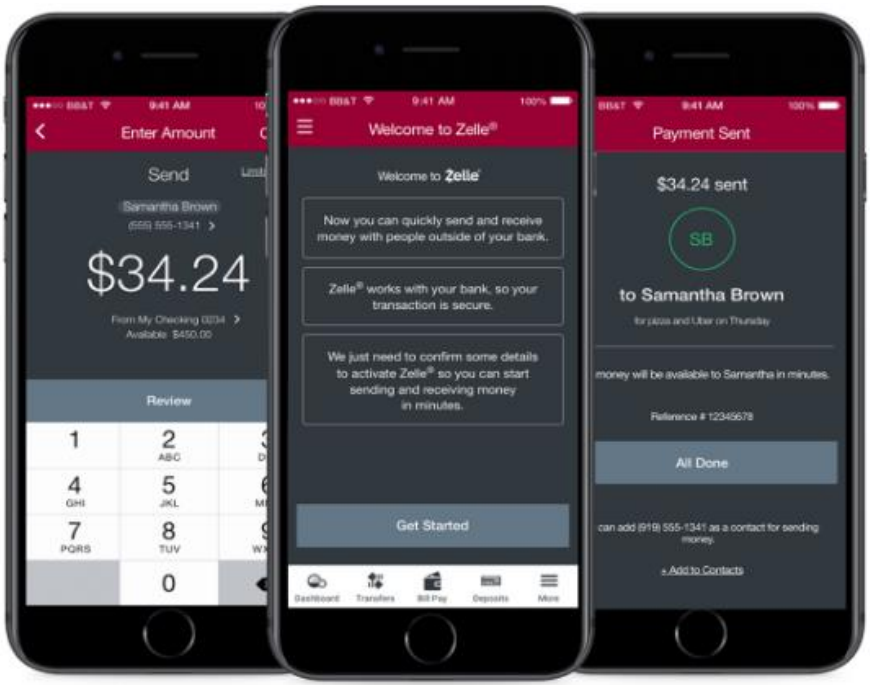
84. Claim 1 of the '455 patent is reproduced below:

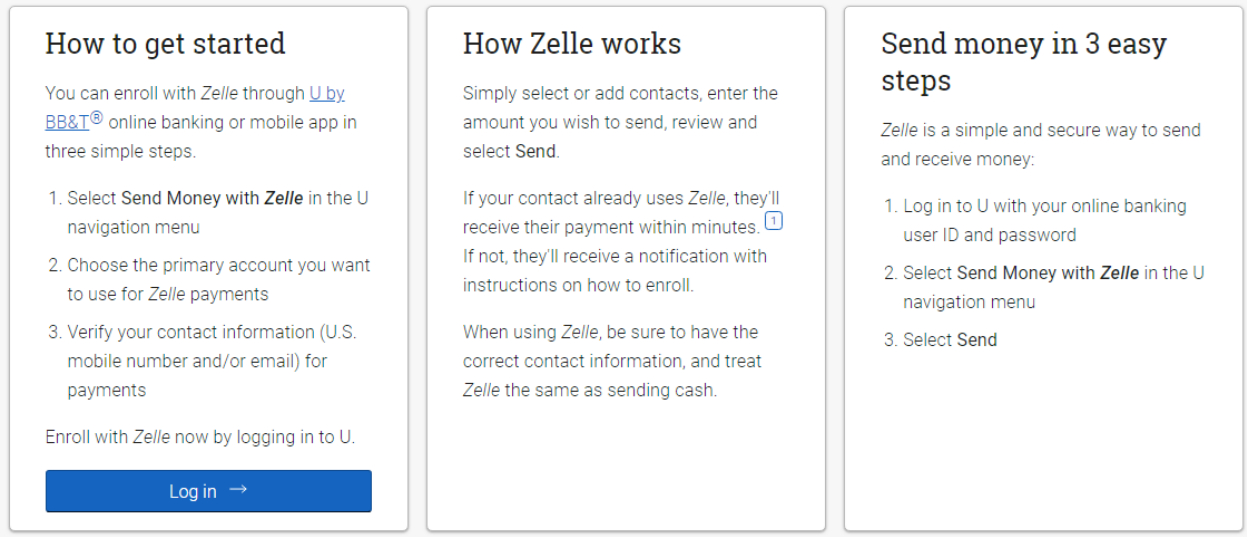
> 1. A method comprising:
>
> receiving, at a server from a client device, one or more messages including a resource identifier, a telephone identifier, and an alias assigned by the server;
>
> transforming, by the server, the telephone identifier and the alias from the message data structure to a database data structure;

authenticating, by the server, the message from the client device by searching for a stored alias and a stored transaction identifier associated with the alias in a database that matches the alias and telephone identifier in the message; and

in response to authenticating the message, authorizing, by the server, a transfer of a resource.

85. BB&T's "U" mobile banking smartphone application in combination with BB&T's backend servers as integrated with the Zelle Alias Directory performs a method comprising receiving from a client device (e.g., mobile phone) one or more messages including a resource identifier (monetary amount), telephone identifier (phone number), and an alias assigned by the server, as illustrated below:





How to get started

You can enroll with *Zelle* through U by BB&T® online banking or mobile app in three simple steps.

1. Select Send Money with ***Zelle*** in the U navigation menu
2. Choose the primary account you want to use for *Zelle* payments
3. Verify your contact information (U.S. mobile number and/or email) for payments

Enroll with *Zelle* now by logging in to U.

Log in →

How Zelle works

Simply select or add contacts, enter the amount you wish to send, review and select **Send**.

If your contact already uses *Zelle*, they'll receive their payment within minutes. [1] If not, they'll receive a notification with instructions on how to enroll.

When using *Zelle*, be sure to have the correct contact information, and treat *Zelle* the same as sending cash.

Send money in 3 easy steps

Zelle is a simple and secure way to send and receive money:

1. Log in to U with your online banking user ID and password
2. Select **Send Money with *Zelle*** in the U navigation menu
3. Select **Send**

Once enrolled, customers can send, request, or receive money with Zelle. To initiate a transaction, users enter the recipient's email address or phone number and the amount to be sent or requested. Users also have the option to add a memo line to the transaction.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

86. BB&T's backend servers as integrated with the Zelle Alias Directory transforms the telephone identifier and alias into a database data structure, and authenticates the message by searching for a stored alias and stored transaction identifier (representation of said transfer) associated with the alias in a database that matches the alias and telephone identifier:

Network Directory—
In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

6. Enrolling in the Service

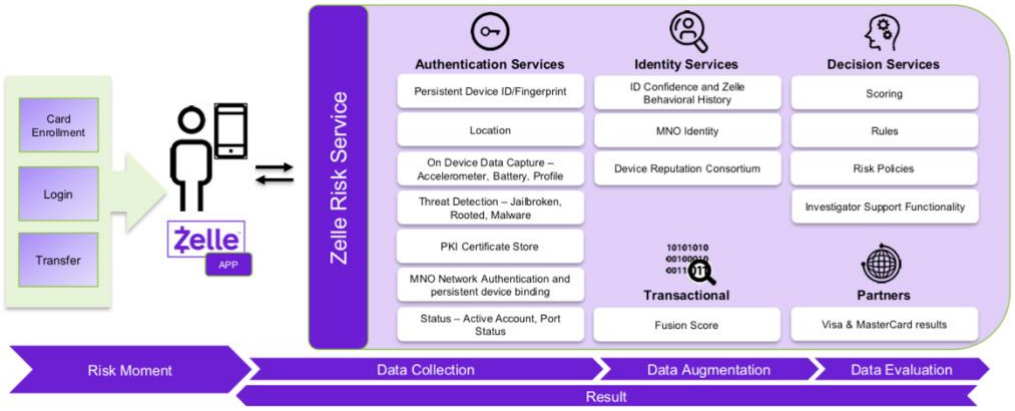
a. You must provide us with an email address that you regularly use and intend to use regularly (i.e., no disposable email addresses) and a permanent mobile phone number that you intend to use for an extended period of time (i.e., no "burner" numbers).

Mobile Phone Number – When shared with us, we collect your mobile number as a means for communicating payment notifications to you and also as a token for authenticating your identity. We also collect the mobile number of any individual which you provide to us for the purpose of facilitating money transfers.

Email Address – We collect your email address when you register an account and to provide you notifications regarding payment transfers and also as a token for authenticating your identity. We also collect the email address of any individual which you provide to us for the purpose of facilitating money transfers.

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

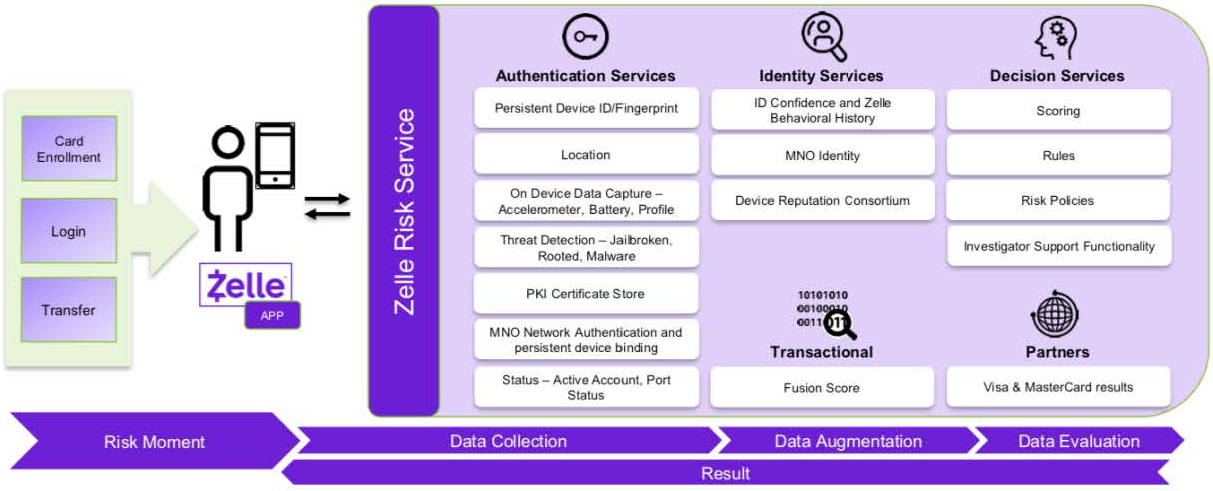


87. Furthermore, BB&T's backend servers as integrated with the Zelle Alias Directory authorize the transfer of the desired amount from the transferor to the transferee in response to authenticating the information from the received message:

Security—
Zelle was developed by the banking industry and benefits from the industry's cybersecurity expertise. Financial institutions in the network do not share customers' account information with each other, so the risk of account information being captured in-flight or at rest is decreased. Customers that access Zelle through their bank's mobile app need provide no sensitive account information. Those who use the standalone app need only share debit card information. The Zelle Alias directory used to facilitate payments only includes the phone numbers and emails associated with Zelle profiles.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

Recipient information refers to information about a recipient used to properly direct payment to the recipient and permit the recipient to identify the correct recipient account.



> With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

88. Additionally, BB&T has been, and currently is, an active inducer of infringement of the '455 patent under 35 U.S.C. § 271(b) and contributory infringement of the '455 patent under 35 U.S.C. § 271(c) literally and/or by the doctrine of equivalents.

89. With knowledge of the '455 patent, BB&T has actively induced, and continues to actively induce, infringement of the '455 patent by intending that others use, offer for sale, or sell in the United States, products and/or services covered by one or more claims of the '455 patent, including but not limited to BB&T's mobile application P2P functionality as integrated with Zelle, and any BB&T product and/or service, alone or in combination, that operates in materially the same manner. BB&T provides such products and/or services to others, such as customers, who, in turn, use, provision for use, offer for sale, or sell in the United States products and/or services that directly infringe one or more claims of the '455 patent.

90. BB&T has actual knowledge of the '455 patent since at least as early as the service upon BB&T of this Complaint. By the time of trial, BB&T will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '455 patent.

91. BB&T has committed, and continues to commit, affirmative acts that cause infringement of one or more claims of the '455 patent with knowledge of the '455 patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims

of the ‘455 patent. BB&T induces such acts of infringement by its affirmative actions of intentionally providing software components that when used in their normal and customary way as desired and intended by BB&T, infringe one or more claims of the ‘455 patent and/or by directly or indirectly providing instructions on how to use its products and/or services in a manner or configuration that infringes one or more claims of the ‘455 patent, including those found at one or more of the following:

- https://www.bbt.com/online-access/online-banking/send-money-with-zelle.html
- https://www.bbt.com/online-access/online-banking/u-by-bbt-video-demos.html
- https://www.bbt.com/online-access/mobile-banking.html
- https://apps.apple.com/us/app/u-digital-banking/id995112030
- https://www.bbt.com/online-access/mobile-banking/mobile-faq.html

92. BB&T has also contributed to, and continues to contribute to, the infringement of the ‘455 patent by others by knowingly providing products and/or services that, when installed and configured result in a system as intended by BB&T, directly infringe one or more claims of the ‘455 patent by a third party, and which have no substantial non-infringing uses, or include a separate and distinct software module described above that is especially made or especially adapted for use in infringement of the ‘455 patent and is not a staple article or commodity of commerce suitable for substantial non-infringing use.

93. As a result of BB&T’s acts of infringement, Plaintiff has suffered and will continue to suffer damages in an amount to be proved at trial.

COUNT IV

(BB&T’s Infringement of U.S. Patent No. 10,127,550)

94. Paragraphs 1-93 are reincorporated by reference as if fully set forth herein.

95. The elements claimed by the '550 patent, taken alone or in combination, were not well-understood, routine or conventional to one of ordinary skill in the art at the time of the invention. Rather, the '550 patent claims and teaches, *inter alia*, an improved system of processing and authenticating, by a server, a TWNP between parties. The invention improved upon then existing transaction authentication methods and systems, which were cumbersome, required extensive disclosure of personal financial information, took several days to process and/or provided insufficient mechanisms by which an originating/target bank could verify individual transactions, with an improved server and aliasing scheme through which party identity and transaction details could be verified and authenticated.

96. The invention further improved upon prior systems and methods by providing a mechanism whereby even a target (e.g., recipient) not previously registered with a payment network could receive transferred funds. This was accomplished by using unique alias information for each party, and a "facilitator" server containing such alias information and other non-sensitive transaction information, which could be used to verify the transaction in near real-time, without an originating bank or customer having to provide sensitive bank account and other financial information to a target bank or customer.

97. In the event of an intended target not being registered with a payment network, the invention teaches a system and method by which the target is notified of the pending transfer and provided instructions to retrieve the transferred funds, again, without disclosing secure financial information outside of the recipient's financial institution.

98. Instead of having to arrange a wire transfer by informing the originating bank of the target's name, bank account number, bank routing number, address, target bank name etc., a consumer or business wishing to transfer funds to a target customer or business simply had to

provide an originator and target alias and other non-sensitive information that could be authenticated by the facilitator server, but that was itself not sensitive financial information that the target/originator wishes to keep confidential. Upon authentication by one or both of the member banks, that bank is provided a guarantee that the transaction was valid, and the funds could be made available substantially immediately, thereby dispensing with the need of sensitive disclosures and complicated and lengthy approval processes.

99. Compared to the prior art, the claimed system for payment authentication and processing is more resilient against fraud because nothing is exchanged during the transaction process that could increase the risk of unauthorized transfers. The alias used to facilitate transfers in Hoss' system, which could be an email address or phone number, by itself cannot be used to facilitate unauthorized transfers. Hoss' system uses an aliasing database which requires only non-sensitive information to be exchanged over the communications network and reconciles transfer details using confidential information that is handled only by the customer's own bank. Such a system is highly resistant to man-in-the-middle attacks and/or spoofing. Thus, Hoss' invention improved TWNP systems by the use of such aliases, allowing for smaller more efficient databases in place of large and disparate institution specific databases, as well as avoiding interoperability issues between previously proprietary transaction systems.

100. The invention represented a technical solution to an unsolved technological problem. The written description of the '550 patent describes, in technical detail, each of the limitations in the claims, allowing a person of skill in the art to understand what those limitations cover, and therefore what was claimed, and to also understand how the non-conventional and non-generic ordered combination of the elements of the claims differ markedly from what had been conventional or generic in the industry at the time of the inventions of the '550 patent.

101. For instance, the claims cover a specific and discrete way to address the problem of reducing fraud and more easily and more securely authenticating transactions in TWNP systems. The invention's solution to this problem is a system that replaces use of private banking information with machine-generated and pre-authenticated aliases to authorize and initiate the transaction directly between financial institutions.

102. More particularly, the inventions disclosed in the '550 patent include transforming non-sensitive user identifying information into an encoded alias which can be efficiently stored in a shared database that is accessible by a number of banks nationwide. The non-sensitive alias information is used by a transferor bank customer (the originator) to identify itself and recipient of transfer requests (e.g., by providing a party alias). When payment is sent to a customer of a bank that has integrated the shared database, the alias is used to authenticate the originator and the recipient by matching the information received by the originator or recipient with the identification stored in the specialized "alias" database. In this manner, financial institutions are assured that the originator and recipient are authorized users. Thereafter, the banks can facilitate the transfer in near real-time, using existing electronic fund transfer technologies, with limited risk that the transaction is fraudulent, and without forcing one customer to share its confidential banking information with the other customer. Moreover, from the user's perspective, the process is unobtrusive, fast and convenient, improving user adoption while still providing increased security. While having wide-ranging implications for the financial industry, the solutions described in the '550 patent are narrowly tailored to the specific fund transfer problems identified above, and thus do not preempt the entire field of securely transferring funds without requiring a transferee customer to share its sensitive financial information with a transferor customer.

103. The claims of the '550 patent each recite a server, comprising a processor, the processor including one or more program modules. Further, the claims of the '550 patent go onto to recite the program modules being configured to send a message to a client device (e.g., recipient mobile phone), wherein the message provides instructions for a target (recipient) to access the server to receive payment; receive one or more messages from the client device, which include an alias (e.g., email address, phone number, name, token, etc.) stored on the server to the target, a transaction identifier assigned by the server identifying a transaction, and a target financial account information (e.g., indication of a "pay-to" account or financial institution); authenticate the one or more messages from the client device by searching for a stored alias and a stored transaction identifier associated with the alias in a database that matches the alias and transaction identifier in the one or more messages; and in response to authenticating, providing instructions to transfer a payment amount from an originator financial account to a target financial account associated with the target financial account information.

104. Certain embodiments of the invention also include providing instructions to another server, in response to authenticating said messages, to initiate transfer of the payment amount from an originator financial account to a target financial account.

105. The system covered by the asserted claims differs markedly from the conventional and generic systems and methods in use at the time of this invention, which *inter alia* lacked the claimed combination of facilitating server, stored alias, stored transaction identifier, instructions for a target to receive the payment, authentication based on matching received and previously stored alias and transaction identifier, and originator financial account and target financial account.

106. The '550 patent is drawn to solving the specific, technical problem of reducing the potential for fraud in TWNP systems while more easily and more securely authenticating the

transaction, particularly in a mobile computing environment and/or over a public communications network, without the disclosure of private banking information. Consistent with the problem addressed being rooted in such TWNP systems, the '550 patent's solutions of replacing private banking information with machine generated, pre-authenticated aliases to facilitate a direct transfer between financial institutions are also rooted in that same technology and cannot be performed with pen and paper or in the human mind. For example, a human cannot use a machine generated alias, which requires a specific sequence of numeric or alpha-numeric characters to identify a desired transferee, never mind authenticate the transaction directly to that transferee's financial institution without requiring the transferee to disclose its private banking information outside of its financial institution.

107. As noted in the patent's specification, the invention's benefits include removing the inherent susceptibility of fraud in communications via public data networks, such as the Internet; reducing the computing power and complexity required for authentication where very large institution specific databases were previously used; and enabling near real-time money transfers directly between financial institutions that maintain private banking networks incapable of integrating with each other.

108. With knowledge of the '550 patent, BB&T has directly infringed, and continues to directly infringe, literally and/or by the doctrine of equivalents, individually and/or jointly, at least claims 1, 10, 12 and 15 of the '550 patent by making, using, testing, selling, offering for sale and/or importing into the United States products and/or services covered by one or more claims of the '550 patent. BB&T's products and/or services that infringe the '550 patent include, but are not limited to, its mobile application P2P payment system referred to as "Send Money with Zelle",

and any other BB&T products and/or services, either alone or in combination, that operate in substantially the same manner.

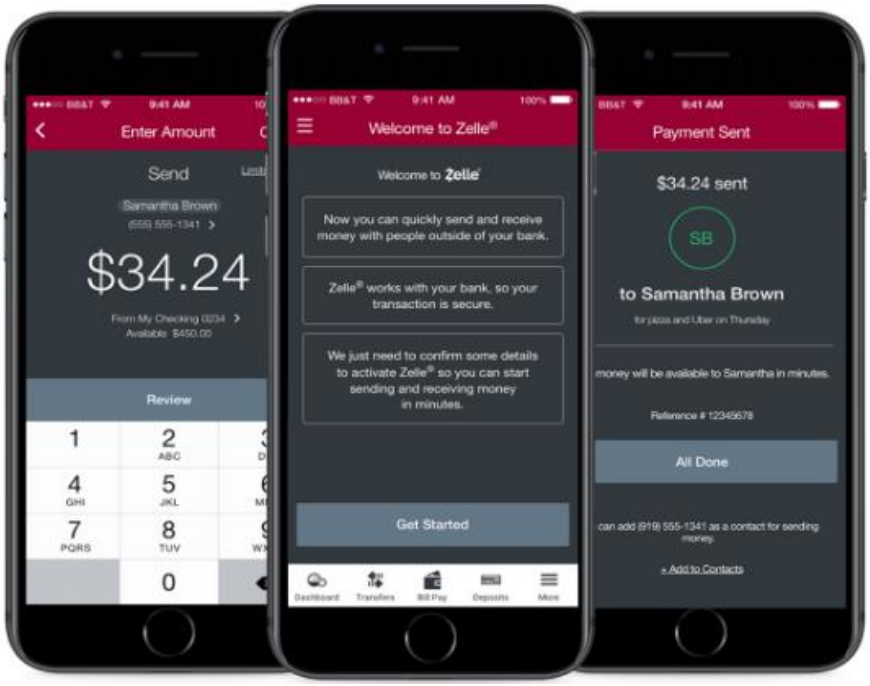
109. Claim 1 of the '550 patent is reproduced below:

> 10. A server comprising:
>
> a processor, the processor including one or more program modules configured to:
>
> send a message to a client device, wherein the message provides instructions for a target to access the server to receive payment;
>
> receive one or more messages from the client device, the one or more messages including an alias stored on the server to the target, a transaction identifier assigned by the server identifying a transaction, and a target financial account information;
>
> authenticate the one or more messages from the client device by searching for a stored alias and a stored transaction identifier associated with the alias in a database that matches the alias and transaction identifier in the one or more messages; and
>
> in response to authentication of the one or more messages from the client device, provide instructions to transfer a payment amount from an originator financial account to a target financial account associated with the target financial account information included in the one or more messages.

110. BB&T's "U" mobile banking smartphone application in combination with BB&T's backend servers as integrated with the Zelle Alias Directory includes a server with a processor and program modules configured to send a message to a client device with instructions to access the server to receive a payment; receive from the client device an alias stored on the server and a transaction identifier and a target financial account information; authenticate by comparing the received alias and transaction identifier with a stored alias and transaction identifier; and provide instructions to transfer the payment from the originating bank account to the target bank account associated with the target financial account information, as claimed in the '550 patent.

111. For example, the BB&T "U" mobile application's "send money with Zelle" P2P payment function provides for an initiating transferor to send funds to a recipient transferee via the BB&T backend servers as integrated with Zelle. The BB&T backend as integrated with Zelle (server including processor and program modules) can operate to send a message with instructions

regarding accessing the server to receive funds (sent via a previously initiated transfer as noted above) to the transferee's client device (e.g., mobile phone) as illustrated below:



How to get started

You can enroll with *Zelle* through U by BB&T® online banking or mobile app in three simple steps.

1. Select Send Money with ***Zelle*** in the U navigation menu
2. Choose the primary account you want to use for *Zelle* payments
3. Verify your contact information (U.S. mobile number and/or email) for payments

Enroll with *Zelle* now by logging in to U.

Log in →

How Zelle works

Simply select or add contacts, enter the amount you wish to send, review and select Send.

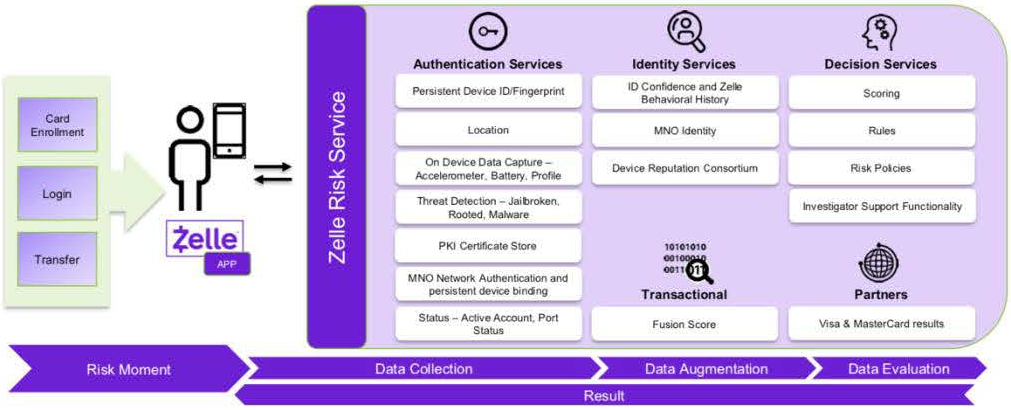
If your contact already uses *Zelle*, they'll receive their payment within minutes. [1] If not, they'll receive a notification with instructions on how to enroll.

When using *Zelle*, be sure to have the correct contact information, and treat *Zelle* the same as sending cash.

Send money in 3 easy steps

Zelle is a simple and secure way to send and receive money:

1. Log in to U with your online banking user ID and password
2. Select Send Money with ***Zelle*** in the U navigation menu
3. Select Send



Will the person I send money to be notified?

Yes! They will receive a notification via email or text message. The message may be sent by *Zelle* or by their bank or credit union.

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

The member bank transmits inquiry to EWS to determine if recipient's token is in a "shared directory."

Assume recipient is not in the directory.

EWS informs the member bank that recipient's token is not in the shared directory. (If recipient is in the directory, payment is available same day, virtually in real time.)

The member bank contacts recipient through the token advising the recipient of the pending transfer by sender and requesting recipient to enroll in the service through recipient's bank (if that bank offers the Zelle payment service) or with EWS.

If recipient banks with a network member bank, recipient may enroll in Zelle through that bank.

112. BB&T's backend servers as integrated with the Zelle Alias Directory receives one or more messages from the client device (e.g., transferee's mobile phone) which includes an alias

for the target, the transaction identifier generated when the transferor submitted the transfer request, and an indication of target financial account information (e.g., whether the target has provided a "pay-to" account or financial institution):

Network Directory—

In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

6. Enrolling in the Service

a. You must provide us with an email address that you regularly use and intend to use regularly (i.e., no disposable email addresses) and a permanent mobile phone number that you intend to use for an extended period of time (i.e., no "burner" numbers).

The member bank transmits inquiry to EWS to determine if recipient's token is in a "shared directory."

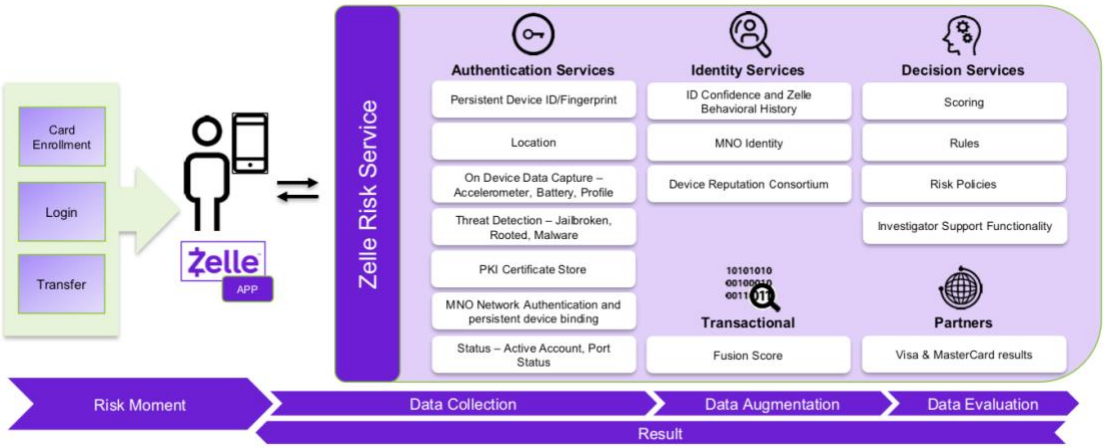
Assume recipient is not in the directory.

EWS informs the member bank that recipient's token is not in the shared directory. (If recipient is in the directory, payment is available same day, virtually in real time.)

The member bank contacts recipient through the token advising the recipient of the pending transfer by sender and requesting recipient to enroll in the service through recipient's bank (if that bank offers the Zelle payment service) or with EWS.

If recipient banks with a network member bank, recipient may enroll in Zelle through that bank.

If you are sending money to someone who has not enrolled as a User with *Zelle*, either in the *Zelle* mobile app or with a Network Financial Institution, they will receive a text message or email notification instructing them on how to enroll with *Zelle* to receive the money. You understand and acknowledge that a



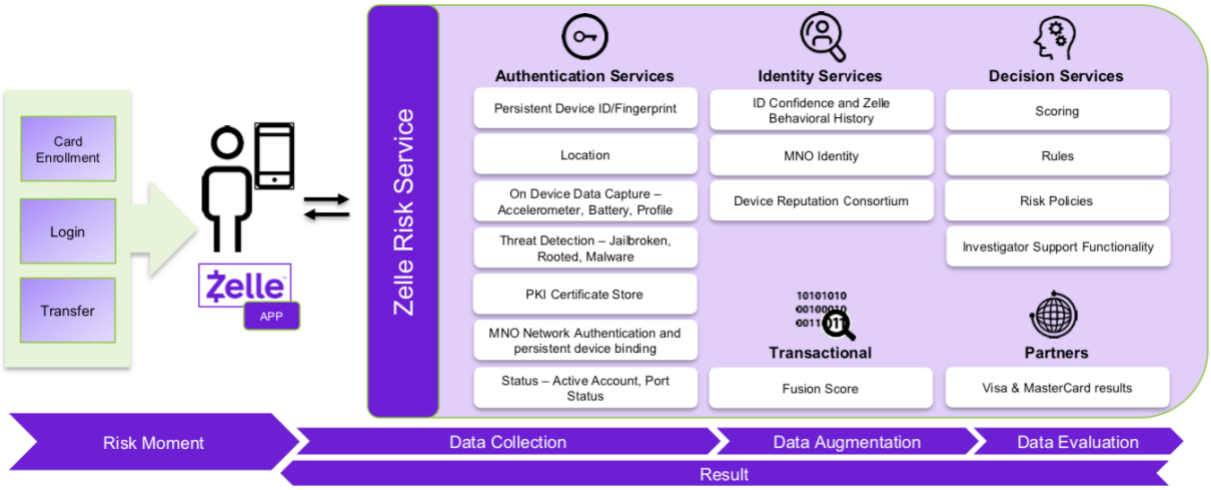
113. Furthermore, the BB&T backend as integrated with the Zelle Alias Directory authenticates the one or more messages from the client device by searching for the alias and transaction identifier in the database that matches the alias and transaction identifier received from the client device:

Security—

Zelle was developed by the banking industry and benefits from the industry's cybersecurity expertise. Financial institutions in the network do not share customers' account information with each other, so the risk of account information being captured in-flight or at rest is decreased. Customers that access Zelle through their bank's mobile app need provide no sensitive account information. Those who use the standalone app need only share debit card information. The Zelle Alias directory used to facilitate payments only includes the phone numbers and emails associated with Zelle profiles.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

Recipient information refers to information about a recipient used to properly direct payment to the recipient and permit the recipient to identify the correct recipient account.



Mobile Phone Number – When shared with us, we collect your mobile number as a means for communicating payment notifications to you and also as a token for authenticating your identity. We also collect the mobile number of any individual which you provide to us for the purpose of facilitating money transfers.

Email Address – We collect your email address when you register an account and to provide you notifications regarding payment transfers and also as a token for authenticating your identity. We also collect the email address of any individual which you provide to us for the purpose of facilitating money transfers.

114. In addition, in response to authentication, the BB&T backend servers as integrated with the Zelle Alias Directory provides instructions to transfer the funds from the originator's

financial account to the target's financial account associated with the target financial account information:

Once enrolled, customers can send, request, or receive money with Zelle. To initiate a transaction, users enter the recipient's email address or phone number and the amount to be sent or requested. Users also have the option to add a memo line to the transaction.

Network Directory—
In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

You may send money to another User at your initiation or in response to that User's request for money. You understand that use of this Service by you shall at all times be subject to (i) this Service Agreement, (ii) your express authorization for a Network Financial Institution to initiate a debit entry to your bank account, and (iii) the terms and conditions of your account agreement with your financial institution. You understand that when you send the payment, you will have no ability to stop it. You

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

Zelle maintains a database of information and through the Service provides the Network Financial Institutions with information necessary to facilitate the transfer of money ("Messages"); however, *Zelle* neither transfers, moves nor initiates the transfer or movement of money. *Zelle*

115. Additionally, BB&T has been, and currently is, an active inducer of infringement of the '550 patent under 35 U.S.C. § 271(b) and contributory infringement of the '550 patent under 35 U.S.C. § 271(c) literally and/or by the doctrine of equivalents.

116. With knowledge of the '550 patent, BB&T has actively induced, and continues to actively induce, infringement of the '550 patent by intending that others use, offer for sale, or sell in the United States, products and/or services covered by one or more claims of the '550 patent, including but not limited to BB&T's mobile application P2P functionality as integrated with Zelle, and any BB&T product and/or service, alone or in combination, that operates in materially the same manner. BB&T provides such products and/or services to others, such as customers, who, in turn, use, provision for use, offer for sale, or sell in the United States products and/or services that directly infringe one or more claims of the '550 patent.

117. BB&T has actual knowledge of the '550 patent since at least as early as the service upon BB&T of this Complaint. By the time of trial, BB&T will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '550 patent.

118. BB&T has committed, and continues to commit, affirmative acts that cause infringement of one or more claims of the '550 patent with knowledge of the '550 patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '550 patent. BB&T induces such acts of infringement by its affirmative actions of intentionally providing software components that when used in their normal and customary way as desired and intended by BB&T, infringe one or more claims of the '550 patent and/or by directly or indirectly providing instructions on how to use its products and/or services in a manner or

configuration that infringes one or more claims of the '550 patent, including those found at one or more of the following:

- https://www.bbt.com/online-access/online-banking/send-money-with-zelle.html
- https://www.bbt.com/online-access/online-banking/u-by-bbt-video-demos.html
- https://www.bbt.com/online-access/mobile-banking.html
- https://apps.apple.com/us/app/u-digital-banking/id995112030
- https://www.bbt.com/online-access/mobile-banking/mobile-faq.html

119. BB&T has also contributed to, and continues to contribute to, the infringement of the '550 patent by others by knowingly providing products and/or services that, when installed and configured result in a system as intended by BB&T, directly infringe one or more claims of the '550 patent by a third party, and which have no substantial non-infringing uses, or include a separate and distinct software module described above that is especially made or especially adapted for use in infringement of the '550 patent and is not a staple article or commodity of commerce suitable for substantial non-infringing use.

120. As a result of BB&T's acts of infringement, Plaintiff has suffered and will continue to suffer damages in an amount to be proved at trial.

COUNT V
(BB&T's Infringement of U.S. Patent No. 10,467,621)

121. Paragraphs 1-120 are reincorporated by reference as if fully set forth herein.

122. The elements claimed by the '621 patent, taken alone or in combination, were not well-understood, routine or conventional to one of ordinary skill in the art at the time of the invention. Rather, the '621 patent claims and teaches, *inter alia*, an improved system to process and authenticate a TWNP between parties. The invention improved upon then existing transaction authentication methods and systems, which were cumbersome, required extensive disclosure of

personal financial information, took several days to process and/or provided insufficient mechanisms by which an originating/target bank could verify individual transactions, with an aliasing scheme through which party identity and transaction details could be verified and authenticated. This was accomplished by using a unique alias to identify a transferee/recipient, transaction identifier, resource identifier, as well as a "facilitator" server containing alias information and other non-sensitive transaction information which could be used to verify the transaction in near real-time, without an originating bank or customer having to provide sensitive bank account and other financial information to a target bank or customer.

123. Instead of having to arrange a wire transfer by informing the originating bank of the target's name, bank account number, bank routing number, address, target bank name etc., a consumer or business wishing to transfer funds to a target customer or business (transferee/recipient) simply had to provide an alias for the originator and target that could be authenticated by the facilitator server, but that was itself not sensitive financial information that the target/originator wishes to keep confidential. Upon authentication by one or both of the member banks, that bank provided a guarantee that the transaction was valid, and the funds could be made available substantially immediately, thereby dispensing with the need for sensitive disclosures and complicated and lengthy approval processes.

124. Compared to the prior art, the claimed system for payment authentication and processing is more resilient against fraud because nothing is exchanged during the transaction process that could increase the risk of unauthorized transfers. The alias used to facilitate transfers in Hoss' system, which could be an email address or phone number for example, by itself cannot be used to facilitate unauthorized transfers. Hoss' system uses an aliasing database which requires only non-sensitive information to be exchanged over the communications network and reconciles

transfer details using confidential information that is handled only by the customer's own bank. Such a system is highly resistant to man-in-the-middle attacks and/or spoofing. Thus, Hoss' invention improved TWNP systems by the use of such aliases, allowing for smaller more efficient databases in place of large and disparate institution specific databases, as well as avoiding interoperability issues between previously proprietary transaction systems.

125. The invention represented a technical solution to an unsolved technological problem. The written description of the '621 patent describes, in technical detail, each of the limitations in the claims, allowing a person of skill in the art to understand what those limitations cover, and therefore what was claimed, and to also understand how the non-conventional and non-generic ordered combination of the elements of the claims differ markedly from what had been conventional or generic in the industry at the time of the inventions of the '621 patent.

126. For instance, the claims cover a specific and discrete way to address the problem of reducing fraud and more easily and more securely authenticating transactions in TWNP systems. The invention's solution to this problem is a system that replaces use of private banking information with machine-generated and pre-authenticated aliases to authorize and initiate the transaction directly between financial institutions.

127. More particularly, the inventions disclosed in the '621 patent include transforming non-sensitive user identifying information into an encoded alias which can be efficiently stored in a shared database that is accessible by a number of banks nationwide. The non-sensitive alias information is used by a transferor bank customer (the originator) to identify itself and recipient of transfer requests (e.g., by providing a party alias). When payment is sent to a customer of a bank that has integrated the shared database, the alias is used to authenticate the originator and the recipient by matching the information received by the originator or recipient with the identification

stored in the specialized "alias" database. In this manner, financial institutions are assured that the originator and recipient are authorized users. Thereafter, the banks can facilitate the transfer in near real-time, using existing electronic fund transfer technologies, with limited risk that the transaction is fraudulent, and without forcing one customer to share its confidential banking information with the other customer. Moreover, from the user's perspective, the process is unobtrusive, fast and convenient, improving user adoption while still providing increased security. While having wide-ranging implications for the financial industry, the solutions described in the '621 patent are narrowly tailored to the specific fund transfer problems identified above, and thus do not preempt the entire field of securely transferring funds without requiring a transferee customer to share its sensitive financial information with a transferor customer.

128. The claims of the '621 patent each recite receiving, at a server from an originator device (e.g., mobile phone), one or more messages identifying an originator alias and a target alias and including instructions to transfer resources from the originator alias to the target alias. Authenticating, by the server, the message(s) by matching the originator alias and the target alias to a plurality of aliases in one or more databases; identifying, by the server, a first payment destination identifier in the database associated with the originator alias and a second payment destination identifier associated with the target alias; and facilitating transfer of the one or more resources from a funding mechanism associated with the first payment destination identifier to an entity associated with the second payment identifier.

129. The system covered by the asserted claims differs markedly from the conventional and generic methods in use at the time of this invention, which *inter alia* lacked the claimed combination of originator and target alias, authenticating base upon matching said aliases with aliases stored in a database, identifying payment destination identifiers associated with the aliases

in the database; and facilitating the transfer of funds from a funding source associated with the first payment identifier to an entity associated with the second payment identifier.

130. The ‘621 patent is drawn to solving the specific, technical problem of reducing the potential for fraud in TWNP systems while more easily and more securely authenticating the transaction, particularly in a mobile computing environment and/or over a public communications network, without the disclosure of private banking information. Consistent with the problem addressed being rooted in such TWNP systems, the ‘621 patent’s solutions of replacing private banking information with machine generated, pre-authenticated aliases to facilitate a direct transfer between financial institutions are also rooted in that same technology and cannot be performed with pen and paper or in the human mind. For example, a human cannot use a machine generated alias, which requires a specific sequence of numeric or alpha-numeric characters to identify a desired transferee, never mind authenticate the transaction directly to that transferee’s financial institution without requiring the transferee to disclose its private banking information outside of its financial institution.

131. As noted in the patent’s specification, the invention’s benefits include removing the inherent susceptibility of fraud in communications via public data networks, such as the Internet; reducing the computing power and complexity required for authentication where very large institution specific databases were previously used; and enabling near real-time money transfers directly between financial institutions that maintain private banking networks incapable of integrating with each other.

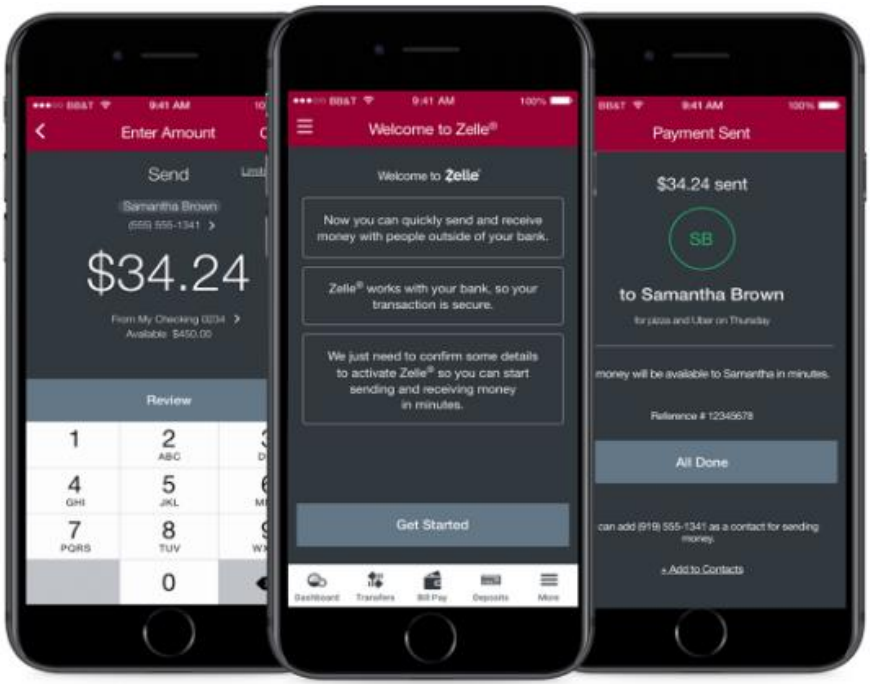
132. BB&T has directly infringed, and continues to directly infringe, literally and/or by the doctrine of equivalents, individually and/or jointly, at least claim 1 of the ‘621 patent by making, using, testing, selling, offering for sale and/or importing into the United States products

and/or services covered by one or more claims of the '621 patent. BB&T's products and/or services that infringe the '621 patent include, but are not limited to, its "U" mobile application P2P payment system referred to as "Send Money with Zelle", and any other BB&T products and/or services, either alone or in combination, that operate in substantially the same manner.

133. Claim 1 of the '621 patent is reproduced below:

> 1. A method comprising:
>
> receiving, at a server, one or more messages from an originator device, the one or more message identifying an originator alias and a target alias, the one or more messages instructing the server to transfer one or more resources from the originator alias to the target alias;
>
> in response to receiving the one or more messages, authenticating, by the server, the one or more messages by matching the originator alias and the target alias to a plurality of aliases in one or more databases, respectively;
>
> in response to the authenticating the one or more messages, identifying, by the server, a first payment destination identifier in the database associated with the originator alias and a second payment destination identifier associated with the target alias; and
>
> facilitating, by the server, transfer of the one or more resources from a funding mechanism associated with the first payment destination identifier to an entity associated with the second payment identifier.

134. BB&T's mobile banking smartphone application in combination with BB&T's backend servers as integrated with the Zelle Alias Directory performs a method comprising receiving, at a server, one or more messages from an originator device, the one or more messages identifying an originator alias and a target alias and instructing the server to transfer a resource from the originator alias to the target alias, as illustrated below:



How to get started

You can enroll with *Zelle* through U by BB&T® online banking or mobile app in three simple steps.

1. Select Send Money with ***Zelle*** in the U navigation menu
2. Choose the primary account you want to use for *Zelle* payments
3. Verify your contact information (U.S. mobile number and/or email) for payments

Enroll with *Zelle* now by logging in to U.

Log in →

How Zelle works

Simply select or add contacts, enter the amount you wish to send, review and select Send.

If your contact already uses *Zelle*, they'll receive their payment within minutes. [1] If not, they'll receive a notification with instructions on how to enroll.

When using *Zelle*, be sure to have the correct contact information, and treat *Zelle* the same as sending cash.

Send money in 3 easy steps

Zelle is a simple and secure way to send and receive money:

1. Log in to U with your online banking user ID and password
2. Select Send Money with ***Zelle*** in the U navigation menu
3. Select Send

Once enrolled, customers can send, request, or receive money with Zelle. To initiate a transaction, users enter the recipient's email address or phone number and the amount to be sent or requested. Users also have the option to add a memo line to the transaction.

expertise. Financial institutions in the network do not share customers' account information with each other, so the risk of account information being captured in-flight or at rest is decreased. Customers that access Zelle through their bank's mobile app need provide no sensitive account information. Those who use the standalone app need only share debit card information. The Zelle Alias directory used to facilitate payments only includes the phone numbers and emails associated with Zelle profiles.

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

As a BB&T client, all you need is U by BB&T account access and your mobile number or email address to take advantage of *Zelle*. Your trusted recipient's email address or U.S. mobile phone number is all you need to send them money.

135. BB&T's backend servers as integrated with the Zelle Alias Directory, in response to receiving the one or more messages, authenticate, by the server, the one or more messages by matching the originator alias and the target alias to a plurality of aliases in one or more databases:

Network Directory—
In-network banks agree to develop and support integration of the Zelle network Shared Directory API, also known as the Alias Directory. Banks are also expected to maintain the relationship of customers' account numbers to their email and mobile number.

6. Enrolling in the Service

a. You must provide us with an email address that you regularly use and intend to use regularly (i.e., no disposable email addresses) and a permanent mobile phone number that you intend to use for an extended period of time (i.e., no "burner" numbers).

Mobile Phone Number – When shared with us, we collect your mobile number as a means for communicating payment notifications to you and also as a token for authenticating your identity. We also collect the mobile number of any individual which you provide to us for the purpose of facilitating money transfers.

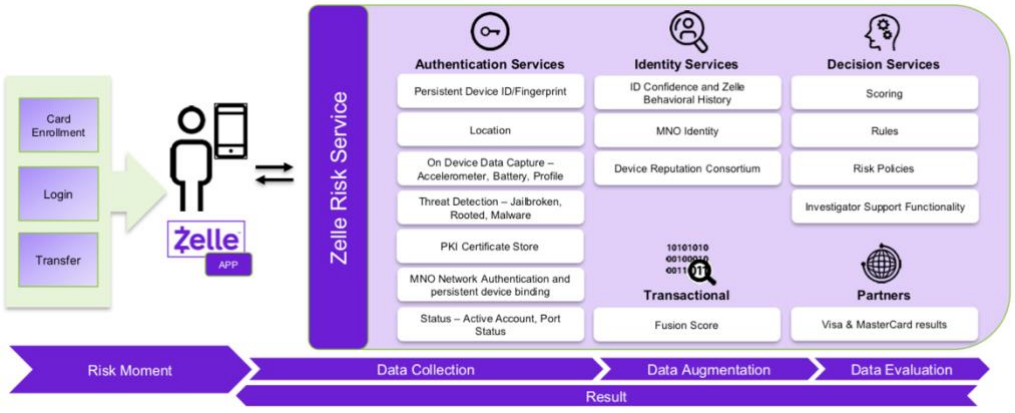
Email Address – We collect your email address when you register an account and to provide you notifications regarding payment transfers and also as a token for authenticating your identity. We also collect the email address of any individual which you provide to us for the purpose of facilitating money transfers.

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

Most transfers of money to you from other Users will occur within minutes. There may be other circumstances when the payment may take longer. For example, in order to protect you, *Zelle* and the Network Financial Institutions, *Zelle* may need additional time to verify your identity or the identity of the person sending the money. We may also delay or block the transfer to prevent

a. BB&T has partnered with the Zelle® Network ("Zelle") to enable a convenient way to transfer money between you and others who are enrolled directly with Zelle or enrolled with another financial institution that partners with Zelle (each, a "User") using aliases, such as email addresses or mobile phone numbers (the "Service"). We will refer to financial institutions that have partnered with Zelle as "Network Banks."

Zelle maintains a database of information and through the Service provides the Network Financial Institutions with information necessary to facilitate the transfer of money ("Messages"); however, *Zelle* neither transfers, moves nor initiates the transfer or movement of money. *Zelle*



136. Furthermore, BB&T's backend servers as integrated with the Zelle Alias Directory, in response to authenticating the one or more messages, identify, by the server, a first payment destination identifier in the database associated with the originator alias and a second payment destination identifier associated with the target alias:

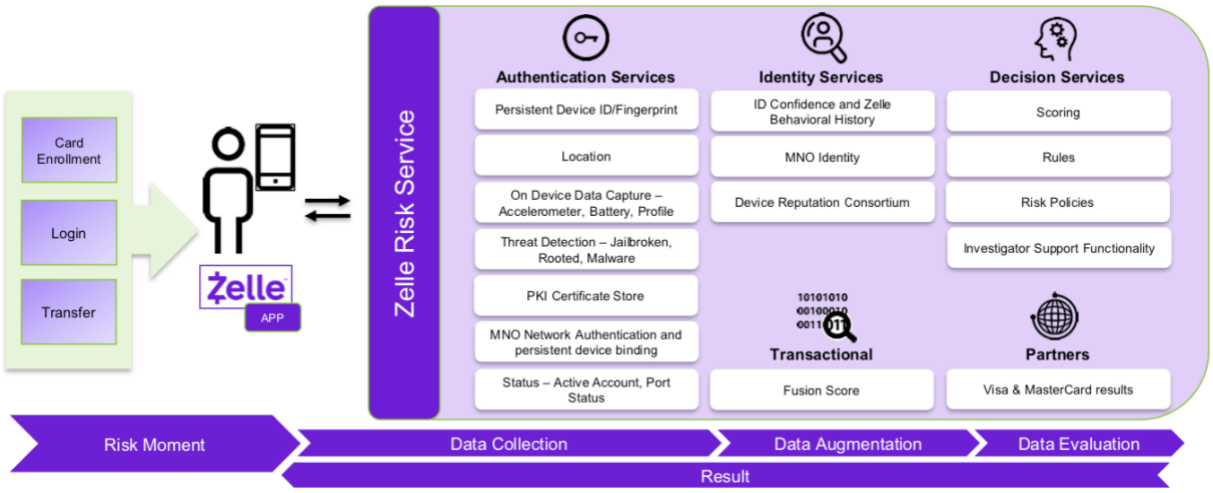
In-Network to In-Network—

If both customers in a Zelle transaction are using in-network banks, the sending bank will conduct a risk assessment of the customers and send the transaction to the Zelle network. Zelle sends a notification to the receiving bank that, through a service level agreement, has five minutes to make the funds available to the recipient. Despite the immediate availability of the funds, settlement takes place over the normal ACH cycle. As was discussed above, banks are responsible for doing the risk assessment on these transactions before they are sent into the network. Once the transaction is sent to Zelle, the sending bank assumes the risk of the transaction.

By matching the enrollment information, EWS now has knowledge that both sender and intended recipient bank with member banks.

(7) Consent to Emails and Automated Text Messages.

By participating as a User in the *Zelle* Service, I represent that I am the owner of the email address, mobile phone number, and/or other alias I registered, or that I have the delegated legal authority to act on behalf of the owner of the email address, mobile phone number, and/or other alias to send or receive money as described in this Addendum. I consent to the receipt of emails or text messages from Bank, from *Zelle* , from other Users that are sending me money or requesting money from me, and from other Network Banks or their agents regarding the *Zelle* Services or related transfers between Network Banks and me. I agree



With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

137. BB&T's backend servers as integrated with the Zelle Alias Directory also, facilitate, by the server, transfer of the one or more resources from a funding mechanism associated with the first payment destination identifier to an entity associated with the second payment identifier:

The process may vary for customers that access Zelle through their bank's mobile app. Customers may be able to change the account associated with their Zelle profile by viewing the setting options within their bank's mobile app. Users can select a different account associated with that financial institution or unregister the phone number or email associated with the account. Customers can contact their bank's customer support team if additional help is needed.

But what tools and systems would be needed to achieve payments in minutes? Innovating on the base capabilities developed by clearXchange, Early Warning created Zelle on an alias-based payment through a shared directory, a set of APIs to enable synchronous and asynchronous operations between participating financial institutions, and a single brand and user experience to be adopted by all participants. The model is a good-funds guarantee model, where the participating financial institutions agree to the same set of network rules and agree to make money available to receiving consumers in minutes, even if the settlement happens on the back end.

With a single brand and user experience, consumers can easily recognize, use and encourage others to use the service. A consumer enrolls with Zelle using the alias or tokenthe recipient's email address or U.S. mobile number. During enrollment, the token is sent via API to the network's shared directory where it is stored along with a bank identification to indicate what FI it is registered with. When payments are sent to a token, the shared directory recognizes the bank ID and routes the payment over an API to the appropriate financial institution where it translates the token to the recipient's bank account and credits the funds within minutes. The token contains no bank account detail.

Zelle maintains a database of information and through the Service provides the Network Financial Institutions with information necessary to facilitate the transfer of money ("Messages"); however, *Zelle* neither transfers, moves nor initiates the transfer or movement of money. *Zelle*

138. Additionally, BB&T has been, and currently is, an active inducer of infringement of the '621 patent under 35 U.S.C. § 271(b) and contributory infringement of the '621 patent under 35 U.S.C. § 271(c) literally and/or by the doctrine of equivalents.

139. With knowledge of the '621 patent, BB&T has actively induced, and continues to actively induce, infringement of the '621 patent by intending that others use, offer for sale, or sell in the United States, products and/or services covered by one or more claims of the '621 patent, including but not limited to BB&T's mobile application P2P functionality as integrated with Zelle, and any BB&T product and/or service, alone or in combination, that operates in materially the same manner. BB&T provides such products and/or services to others, such as customers, who, in turn, use, provision for use, offer for sale, or sell in the United States products and/or services that directly infringe one or more claims of the '621 patent.

140. BB&T has actual knowledge of the '621 patent since at least as early as the service upon BB&T of this Complaint. By the time of trial, BB&T will have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '621 patent.

141. BB&T has committed, and continues to commit, affirmative acts that cause infringement of one or more claims of the '621 patent with knowledge of the '621 patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '621 patent. BB&T induces such acts of infringement by its affirmative actions of intentionally providing software components that when used in their normal and customary way as desired and intended by BB&T, infringe one or more claims of the '621 patent and/or by directly or indirectly providing instructions on how to use its products and/or services in a manner or

configuration that infringes one or more claims of the ‘621 patent, including those found at one or more of the following:

- https://www.bbt.com/online-access/online-banking/send-money-with-zelle.html
- https://www.bbt.com/online-access/online-banking/u-by-bbt-video-demos.html
- https://www.bbt.com/online-access/mobile-banking.html
- https://apps.apple.com/us/app/u-digital-banking/id995112030
- https://www.bbt.com/online-access/mobile-banking/mobile-faq.html

142. BB&T has also contributed to, and continues to contribute to, the infringement of the ‘621 patent by others by knowingly providing products and/or services that, when installed and configured result in a system as intended by BB&T, directly infringe one or more claims of the ‘621 patent by a third party, and which have no substantial non-infringing uses, or include a separate and distinct software module described above that is especially made or especially adapted for use in infringement of the ‘621 patent and is not a staple article or commodity of commerce suitable for substantial non-infringing use.

143. As a result of BB&T’s acts of infringement, Plaintiff has suffered and will continue to suffer damages in an amount to be proved at trial.

PRAYER FOR RELIEF

Plaintiff requests that the Court enter judgment against BB&T:

(A) that BB&T has infringed one or more claims of each of the above patents-in-suit, directly and/or indirectly, literally and/or under the doctrine of equivalents;

(B) awarding damages sufficient to compensate Plaintiff for BB&T's infringement under 35 U.S.C. § 284;

(C) enjoining BB&T's infringement of the patents-in-suit;

(D) finding this case exceptional under 35 U.S.C. § 285 and awarding Plaintiff its reasonable attorneys' fees;

(E) awarding Plaintiff its costs and expenses incurred in this action;

(F) awarding Plaintiff prejudgment and post-judgment interest; and

(G) granting Plaintiff such further relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands trial by jury of all claims so triable under Federal Rule of Civil Procedure 38.

Date: November 6, 2019

Respectfully submitted,

/s/ Derek Gilliland
DEREK GILLILAND
State Bar No. 24007239
Of Counsel
SOREY LAW FIRM, PLLC
109 W. Tyler St.
Longview, TX 75601
903.212.2822 (Telephone)
derek@soreylaw.com

KARL RUPP
State Bar No. 24035243
NIX PATTERSON, LLP
1845 Woodall Rodgers Fwy., Suite 1050
Dallas, TX 75201
972.831.1188 (Telephone)
972.444.0716 (Facsimile)
krupp@nixlaw.com

OF COUNSEL:

PAUL J. HAYES
phayes@princelobel.com
MATTHEW VELLA
mvella@princelobel.com
ROBERT R. GILMAN
rgilman@princelobel.com
JONATHAN DEBLOIS
jdeblois@princelobel.com
ALEX BREGER
abreger@princelobel.com
PRINCE LOBEL TYE LLP
One International Place, Suite 3700
Boston, MA 02110
Tel: (617) 456-8000
Fax: (617) 456-8100

COUNSEL for PLAINTIFFS